De rol van Internet Service Providers bij de bestrijding van botnets

Naam afstudeerder	: Jeroen Pijpker
Studentnummer	: 851241385
Datum eindpresentatie	: 19 november 2015

The role of Internet Service Providers in botnet mitigation

Naam afstudeerder	: Jeroen Pijpker
Studentnummer	: 851241385
Opleiding	: Masteropleiding Business Process Management and IT
Faculteit	: Faculteit Management, Science & Technology
Universiteit	: Open Universiteit
Cursuscode	: T9232B
Datum	: 8 november 2015
1e begeleider & examinator	: dr. ir. H.P.E. (Harald) Vranken
2e begeleider	: dr. ir. A.J.F (Arjan) Kok

Voorwoord

Met het schrijven van mijn afstudeerscriptie komt er een einde aan mijn masteropleiding Business Process Management & IT. Ik heb bewust een keuze gemaakt om een onderzoek te doen binnen de IT security, omdat dit onderwerp binnen mijn dagelijkse werkzaamheden als docent een steeds belangrijkere rol speelt. Daarnaast ben ik er persoonlijk van overtuigd dat er steeds meer waarde wordt gehecht aan een goede beveiliging van apparaten die zijn aangesloten op het internet. Na het afsluiten van mijn studie is het de bedoeling om mijzelf op dit vakgebied verder te ontwikkelen.

Ter oriëntatie inzake het onderwerp botnets heb ik een aantal congressen bezocht. Zo ben ik onder andere afgereisd naar Polen om daar een congres bij te wonen van 'The Honeynet Project'. Tijdens dit congres heb ik een aantal workshop gevolgd op het gebied van botnets.

Mijn dank gaat uit naar de organisaties die hebben meegewerkt aan mijn onderzoek. Helaas kan ik de personen niet noemen in verband met de vertrouwelijkheid van de interviews. Ik kijk met plezier terug op de interviews en de interessante discussies die zijn gevoerd met betrekking tot botnetbestrijding.

Natuurlijk wil ik ook mijn werkgever bedanken voor het geven van de mogelijkheid om verder te studeren. Dit was één van mijn grote wensen toen ik in 2008 de overstap maakte naar het onderwijs.

Ik wil Harald Vranken bedanken voor zijn begeleiding tijdens het afstudeeronderzoek. Zijn opbouwende commentaar en kennis hebben mij enorm geholpen tijdens het onderzoek. Tijdens de verschillende (prettige) bespreekmomenten heeft Harald de juiste sturing gegeven aan het onderzoek zodat ik weer een stap kon maken in de goede richting.

Tot slot wil ik mijn vrouw Karin bedanken. Zij heeft mij de afgelopen jaren bijgestaan en mij de mogelijkheid gegeven om de studie aan de Open Universiteit te volgen.

Jeroen Pijpker

Valthe, 8 november 2015

Inhoudsopgave

Lijst van tabellen

Lijst van figuren

Samenvatting

Steeds vaker wordt er in het nieuws melding gemaakt van cybercriminaliteit. Cybercriminaliteit is een steeds groter probleem in onze samenleving. Daarbij maken cybercriminelen in steeds meer gevallen gebruik van een speciaal soort malware, namelijk botnets. Botnets zijn netwerken van geïnfecteerde apparaten (bots) die onder controle staan van een zogenaamde botmaster en gecoördineerd aanvallen op andere apparaten kunnen uitvoeren. In meerdere wetenschappelijke publicaties wordt aangegeven dat Internet Service Providers (hierna: ISP's) een belangrijke rol kunnen spelen bij de bestrijding van botnets. Dit onderzoek richt zich op de problematiek rond botnetbestrijding door ISP's.

De centrale onderzoeksvraag die wordt beantwoord binnen dit afstudeeronderzoek is de volgende:
'Welke rol spelen Internet Service Providers bij de bestrijding van botnets op technisch gebied, hoe pakken ze dit organisatorisch aan en wat zijn juridisch gezien de mogelijkheden en beperkingen?'

Het onderhavige onderzoek is uitgevoerd in een theoretisch en empirisch deel. Het doel van het theoretisch deel is op basis van een literatuuronderzoek een conceptueel model en theoretisch referentiemodel op te stellen die weergeven hoe botnetbestrijding door ISP's is georganiseerd op technisch gebied, hoe ze dit organisatorisch aanpakken en welke bevoegdheden ze juridisch hebben. Voor het theoretische deel zijn zeven onderzoeksvragen opgesteld. De eerste drie theoretische onderzoeksvragen richten zich op botnets, de eigenschappen van botnets en hoe ze kunnen worden gedetecteerd en bestreden. In de daarop volgende drie theoretische onderzoeksvragen is gekeken naar de rol van ISP's bij botnetbestrijding, welke juridische verantwoordelijkheden (rechten en plichten) hebben ISP's in relatie tot botnetbestrijding en wat doen de ISP's afzonderlijk van elkaar aan botnetbestrijding. In de laatste theoretische onderzoeksvraag is onderzocht welke samenwerkingsverbanden en initiatieven in de literatuur bekend zijn met betrekking tot botnetbestrijding.

Dit heeft geresulteerd in een conceptueel model en in een referentiemodel. Het referentiemodel geeft weer hoe volgens de wetenschappelijke literatuur botnetbestrijding door ISP's wordt uitgevoerd. Het referentiemodel is opgedeeld in vijf verschillende hoofdgebieden. Deze hoofdgebieden vormen samen de anti-botnet life cycle. De stappen die een ISP kan uitvoeren volgens de anti-botnet life cycle zijn het nemen van preventieve maatregelen, detectie van botnets, informeren van betrokken partijen, oplossen van een botnetbesmetting en ondersteunen bij herstel na een besmetting.

Vervolgens is in het empirische gedeelte van het onderzoek getoetst of het theoretisch referentiemodel overeenkomt met de wijze waarop Nederlandse ISP's botnets bestrijden. Voor het empirisch onderzoek is een aantal onderzoeksvragen opgesteld die, samen met het referentiemodel, door middel van semigestructureerde interviews zijn getoetst bij de betrokken ISP's en het Nationaal Cyber Security Centrum (NCSC).

Uit de interviews blijkt dat de betrokken partijen zich herkennen in het referentiemodel. Er zijn door hen geen ontbrekende aspecten geconstateerd. Op basis van de uitwerkingen van

de interviews zijn er wijzigingen doorgevoerd in het referentiemodel. De belangrijkste wijziging in het referentiemodel is het verwijderen van de aspecten met betrekking tot actief meekijken in het klantverkeer. Door alle geïnterviewde organisaties, die actief zijn in de particuliere markt, is aangegeven dat er niet actief meegekeken wordt in het klantverkeer. Zogenaamde Intrusion Prevention System (IPS) en Intrusion Detection System (IDS) worden door ISP's niet ingezet. Informatie die ISP's verwerken met betrekking tot botnetinfecties, komt niet tot stand door mee te kijken in het verkeer van de klant. Wat verder uit de interviews naar voren komt, is dat alle providers zich bewust zijn van hun zorgplicht richting hun klanten.

De hoofdvraag van dit onderzoek is welke rol ISP's spelen bij de bestrijding van botnets. De conclusies die uit onderhavig onderzoek kunnen worden getrokken, zijn:
Door de ISP's binnen Nederland wordt bijgedragen aan het mitigeren van botnets. De ISP's doen dit binnen de vijf gebieden van de anti-botnet life cycle. Volgens artikel 11.3 van telecommunicatiewet zijn ISP's juridisch verplicht om organisatorisch en technische maatregelen te nemen om hun klanten te beschermen tegen internetcriminaliteit. Echter, in het definitieve referentiemodel valt op dat weinig aspecten juridisch van aard zijn. Het merendeel van de aspecten binnen het definitieve referentiemodel zijn organisatorisch van aard. Vier van de vijf ISP's zijn actief in een samenwerkingsverband om botnets te bestrijden. Door de ISP's wordt de informatie inzake botnetbesmettingen ontvangen van externe bronnen (bijvoorbeeld: AbuseHub). Informatie over mogelijke besmettingen komt niet tot stand door actieve monitoring van het netwerkverkeer. Door de ISP's, die actief zijn in de particuliere markt, wordt nadrukkelijk aangegeven dat informatie over mogelijke bots binnen hun netwerk niet door actieve monitoring tot stand komt.

ISP's zijn zich bewust van hun rol in botnetbestrijding in relatie tot hun rechten en plichten. Echter, de ISP's richten zich met name op de individuele bots die actief zijn bij klanten binnen hun netwerk. ISP's zijn in mindere mate betrokken bij initiatieven tegen botnets als geheel.

Het definitieve referentiemodel geeft een duidelijk beeld hoe botnetbestrijding door ISP's is georganiseerd. Daarnaast kan het model gebruikt worden om te bepalen waar door ISP's initiatieven kunnen worden ontplooit om botnets nog beter te mitigeren.

Als algehele conclusie kan gesteld worden dat de hoofdvraag in dit onderzoek is beantwoord. Het is duidelijk geworden dat ISP's een (belangrijke) rol spelen bij botnetbestrijding en zich bewust zijn van de gevaren van botnets.

1 Inleiding

1.1 Aanleiding tot het onderzoek

In het nieuws wordt steeds vaker melding gemaakt van cybercriminaliteit. Daarbij maken cybercriminelen in steeds meer situaties gebruik van een speciaal soort malware, namelijk botnets (Nationaal Cyber Security Centrum, 2014). Botnets zijn netwerken van geïnfecteerde apparaten (bots) die onder controle staan van een zogenaamde botmaster en gecoördineerd aanvallen op andere apparaten kunnen uitvoeren. Botnets worden onder andere ingezet door (cyber)criminelen om zichzelf te verrijken. Daarnaast zijn er ook situaties waar botnets om politieke redenen worden ingezet.

In meerdere onderzoeken wordt aangegeven dat botnets op dit moment één van de grootste bedreigingen zijn op het internet (Edwards, 2011; van Eeten, Bauer, Asghari, & Tabatabaie, 2010). In het Cybersecuritybeeld van 2013 voor Nederland wordt aangegeven dat botnets de grootste cyberbedreiging vormen in Nederland (Nationaal Cyber Security Centrum, 2013). In het daarop volgende Cybersecuritybeeld van 2014 wordt aangegeven dat het gebruik van botnets winstgevender wordt voor de cybercriminelen en dat botnets steeds beter worden verhuld en verdedigd (Nationaal Cyber Security Centrum, 2014).

Bij de bestrijding van botnets zijn private en publieke organisaties betrokken. Een belangrijke private partij bij de bestrijding van botnets zijn de Internet Service Providers (hierna: ISP's) (Opstelten, 2014). De traditionele rol van ISP's is het voorzien van klanten van internettoegang en het (internet)verkeer van de klanten te behandelen volgens de netneutraliteitrichtlijnen. In dit onderzoek wordt de volgende definitie gehanteerd voor een Internet Service Provider (hierna: ISP):
Een Internet Service Provider is een organisatie die individuen en organisaties van internet voorziet (van Eeten & Bauer, 2008).

Uit meerdere wetenschappelijke artikelen komt naar voren dat ISP's een belangrijke rol kunnen spelen bij botnetbestrijding (Moore, Clayton, & Anderson, 2009; Silva, Silva, Pinto, & Salles, 2013). Wat in de literatuur minder naar voren komt, is de wijze waarop ISP's botnetbestrijding aanpakken. In verschillende literatuur en zogenaamde 'best practices' worden wel voorstellen gedaan omtrent de aanpak van botnetbestrijding door ISP's. Echter, in de literatuur is er nagenoeg geen informatie te vinden wat de resultaten hiervan zijn. Dit onderzoek wil een bijdrage leveren aan de theorievorming over de rol van ISP's bij botnetbestrijding.

1.2 Internet Service Providers

Het Centraal Bureau voor de Statistiek (2014) rapporteerde in hun jaarlijkse uitgave 'ICT kennis en Economie 2014' over het feit dat vrijwel iedere Nederlander toegang tot internet heeft. Dit kan zijn via een vaste verbinding of onderweg via mobiele verbindingen. In Nederland hebben vrijwel alle huishoudens technisch gezien de mogelijkheid om een vaste breedbandaansluiting te nemen (kabel, DSL of glasvezel). Volgens het Centraal Bureau voor de statistiek had in 2013 95 procent van de Nederlandse huishouden toegang tot internet (Centraal Bureau voor de

Statistiek [CBS], 2013). DSL en kabel zijn de meest gebruikte vormen van breedband in Nederland. In 2013 verliep 48 procent van de breedbandaansluitingen via DSL en 45 procent via de kabel.

Elk kwartaal wordt door de Autoriteit Consument & Markt de telecommonitor gepubliceerd waarin de marktcijfers van de telecomsector zijn opgenomen. De telecommonitor laat de ontwikkelingen zien op het gebied van breedbandinternet op basis van cijfers van de belangrijkste partijen in de telecomsector. In de telecommonitor van het tweede kwartaal van 2014, die is gepubliceerd op 21 november 2014, zijn de marktaandeelcijfers breedband per aanbieder opgenomen (Autoriteit Consument & Markt [ACM], 2014). In Tabel 1 is de procentuele verdeling in marktaandeel opgenomen tussen de verschillende 'grote' providers.

Tabel 1 Marktaandeelcijfers breedband

	30-9-2012	31-12-2012	31-3-2013	30-6-2013	30-9-2013	31-12-2013	31-3-2014	30-6-2014
CANALDIGITAAL	-	-	-	-	-	-	[0 - 5%]	[0 - 5%]
KPN	[40 - 45%]	[40 - 45%]	[40 - 45%]	[40 - 45%]	[40 - 45%]	[40 - 45%]	[40 - 45%]	[40 - 45%]
TELE2	[5 - 10%]	[5 - 10%]	[5 - 10%]	[5 - 10%]	[5 - 10%]	[0 - 5%]	[0 - 5%]	[0 - 5%]
T-MOBILE	[0 - 5%]	[0 - 5%]	[0 - 5%]	[0 - 5%]	[0 - 5%]	[0 - 5%]	-	-
UPC	[15 - 20%]	[15 - 20%]	[15 - 20%]	[15 - 20%]	[15 - 20%]	[15 - 20%]	[15 - 20%]	[15 - 20%]
ZIGGO	[25 - 30%]	[25 - 30%]	[25 - 30%]	[25 - 30%]	[25 - 30%]	[25 - 30%]	[25 - 30%]	[25 - 30%]
Overig	[5 - 10%]	[5 - 10%]	[5 - 10%]	[5 - 10%]	[0 - 5%]	[5 - 10%]	[5 - 10%]	[5 - 10%]

Wat opvalt in deze tabel is het marktaandeel van de drie grote providers, namelijk KPN, UPC en Ziggo. Daarnaast zijn UPC en Ziggo gefuseerd.

In de literatuur wordt er door Salemink en Strijker (2012) een bruikbare definitie gegeven van breedband, namelijk:
Breedbandnetwerken zijn toekomstbestendige next generation access netwerken die verbindingen ondersteunen met een capaciteit van 100 mbit/s symmetrisch, waarbij meer capaciteit tegen geringe kosten realiseerbaar is.

In Tabel 1, met daarin de marktaandeelcijfers breedband, is er een groep overige. Dit zijn merendeels kleine lokale partijen, zoals bijvoorbeeld Zeelandnet en Solcon, die breedbandaansluitingen leveren.

In de telecommonitor worden niet alle ISP's meegenomen, omdat de telecommonitor zich richt op ISP's die leveren aan consumenten. Binnen Nederland zijn er nog andere ISP's actief die bijvoorbeeld diensten leveren aan het onderwijs of bedrijven. Een voorbeeld hiervan is SURFnet. SURFnet is namelijk de ISP voor wetenschappelijk onderzoek, hoger onderwijs en voor andere OCW-gefinancierde instellingen. Scholen voor primair en voortgezet onderwijs en culturele instellingen kunnen via serviceproviders gebruik maken van het netwerk van SURFnet. Op de website van SURFnet is een lijst met aangesloten instellingen te vinden waaraan SURFnet haar diensten levert (SURFnet, 2015). Binnen SURFnet wordt actief onderzoek gedaan naar cybercriminaliteit.

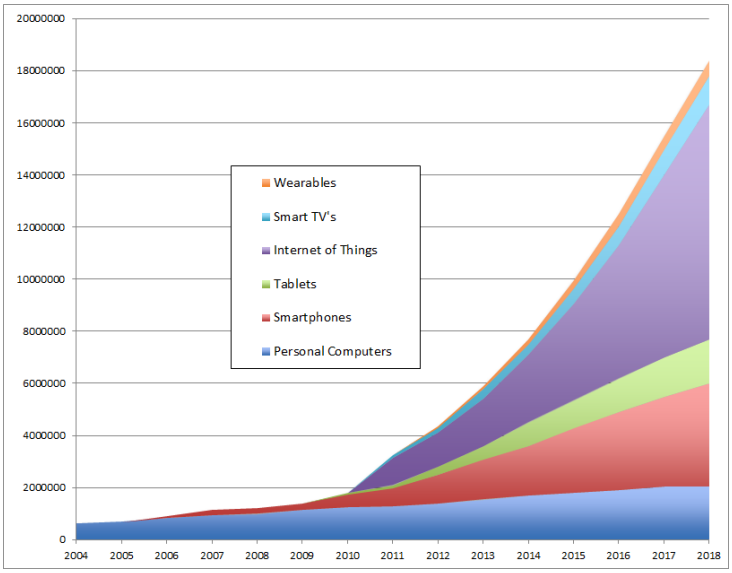
1.3 Botnets

Als er in de literatuur op zoek wordt gegaan naar een definitie voor een botnet valt het op dat in de omschrijving voor wat een botnet is het woord "malicious" (kwaadaardig) meestal wordt

genoemd. Malicious wordt vaak in één adem genoemd met botnet, terwijl dit niet het geval hoeft te zijn. Het eerste botnet, die Eggdrop werd genoemd, werd in 1993 ontwikkeld. Eggdrop had als taak het assisteren in IRC channel management. Hieruit kan geconcludeerd worden dat een botnet niet per definitie kwaadaardig hoeft te zijn. Echter, dit onderzoek richt zich alleen op de kwaadaardige varianten van botnets.

In de literatuur wordt nagenoeg een eenduidige definitie voor het begrip botnet gebruikt. Zoals Schless (2013) aangeeft zit het verschil alleen in de bewoordingen. De meeste auteurs beschouwen botnets als netwerken van schadelijke software (malware) op gehackte of geïnfecteerde computers die onder controle van een persoon of organisatie staan.

In dit onderzoek is er voor gekozen om in de definitie van een botnet de term computers te vervangen door hosts of machines. Hiervoor is gekozen, omdat malware tegenwoordig op allerlei apparaten voorkomt, zoals bijvoorbeeld smartphones. Zo werd er op 19 januari 2014 melding gemaakt dat koelkasten, die met internet waren verbonden, onderdeel uit maakten van een botnet(CNET, 2014). De verwachting is dat door een toename van apparaten die verbinding maken met internet, ook malware op deze devices zal toenemen. Dit blijkt ook uit onderzoek van Business Insider over 'the internet of things' waaruit blijkt dat er een explosieve groei is (zie Figuur 1) van devices/apparaten die worden verbonden met het internet. De verwachting is dat deze groei de komende 12 tot 15 jaar zal aanhouden. Het is de verwachting dat daarna standaard alle devices/apparaten verbonden zijn met het internet.



Figuur 1 Groei internet of things (Business Insider, 2013)[1]

In dit onderzoek is er voor gekozen om de volgende definitie voor botnets te hanteren:

> ***Botnets zijn netwerken van samenwerkende apparaten die zijn geïnfecteerd (onvrijwillig) met (dezelfde) malware en onder controle staan van een persoon of organisatie en gecoördineerd cyberaanvallen kunnen uitvoeren.***

[1] Figuur 1 laat de groei van apparaten zien die verbonden worden met het internet. Een gedeelte van deze apparaten vallen binnen een bepaalde groep (bijvoorbeeld SmartTV's). Echter, er is een groep van nog niet benoemde apparaten. Deze groep is in Figuur 1 aangegeven in het paars.

Het verschil tussen botnets en 'standaard' malware is dat er bij botnets een communicatiestructuur bestaat genaamd 'Command and Control (C&C of C2)' (Zeidanloo & Manaf, 2009). In een botnet communiceren de verschillende bots met een C&C server of door middel van peers.

1.4 Opzet afstudeerrapport

Het afstudeeronderzoek is gefaseerd uitgevoerd. Namelijk, een theoretisch gedeelte en een empirisch gedeelte. In het theoretisch gedeelte is er een literatuuronderzoek uitgevoerd dat als resultaat een referentiemodel heeft opgeleverd. Dit theoretisch referentiemodel is vervolgens empirisch getoetst.

Hieronder in Tabel 2 is de opzet van het afstudeerverslag op hoofdonderdelen weergegeven.

Tabel 2 Structuur afstudeerrapport

Hoofdstuk	Onderdeel
1. Inleiding	Aanleiding
2. Methode van onderzoek	Probleemstelling, onderzoeksvragen, conceptueel onderzoeksmodel, methode van onderzoek voor het theoretisch gedeelte en methode van onderzoek voor het empirisch gedeelte
3. Botnetbestrijding door ISP's	Uitwerking literatuuronderzoek
4. Conceptueel model en referentiemodel	Conceptueel model, Referentiemodel
5. Empirische onderzoeksvragen	Uitwerking onderzoeksvragen, definitief referentiemodel
6. Conclusie en aanbevelingen	Conclusie aanbevelingen

1.5 Engels

In dit afstudeerverslag is er voor gekozen om een aantal Engelse termen waar nodig te vertalen naar het Nederlands. Echter, dit is niet voor alle Engelse termen gedaan in verband met de leesbaarheid van het afstudeerverslag. Er is dus bewust een keuze gemaakt om af en toe de Engelse bewoording niet te vertalen, omdat dit afbreuk zou doen aan de leesbaarheid.

2 Methode van onderzoek

In dit hoofdstuk wordt de onderzoeksaanpak uiteengezet. Allereerst wordt er begonnen met de probleemstelling van het afstudeeronderzoek en vervolgens worden de onderzoeksvragen gepresenteerd. Daarna wordt het onderzoeksmodel weergegeven en wordt het soort onderzoek verklaard.

Voor het beantwoorden van de onderzoeksvragen is er een literatuurstudie uitgevoerd. De verantwoording van deze aanpak is opgenomen in dit hoofdstuk. In dit hoofdstuk is tot slot de verantwoording van de aanpak het empirisch deel opgenomen.

2.1 Probleemstelling

De probleemstelling van het afstudeeronderzoek wordt gevormd door de doelstelling en de vraagstelling van het onderzoek.

2.1.1 Doelstelling

In paragraaf 1.1 zijn de achtergronden van het afstudeeronderzoek geschetst. De hoofddoelstelling van het afstudeeronderzoek is hierop gebaseerd:

'Het doel van het afstudeeronderzoek is vaststellen welke rol Internet Services Providers op dit moment spelen bij de bestrijding van botnets in Nederland.'

Zoals aangegeven in paragraaf 1.4 is het onderzoek uitgevoerd in twee delen. Namelijk een theoretisch deel (literatuuronderzoek) en een empirisch deel. Naast de hoofddoelstelling is er voor het theoretisch deel en het empirisch deel afzonderlijk een subdoelstelling gedefinieerd. De doelstelling voor het literatuuronderzoek luidt als volgt:

'Het literatuuronderzoek heeft tot doel een conceptueel model/referentiemodel op te stellen dat weergeeft hoe botnetbestrijding door Internet Service Providers is georganiseerd op technisch gebied, hoe ze dit organisatorisch aanpakken en welke bevoegdheden ze juridisch hebben.'

De doelstelling voor het empirisch gedeelte luidt als volgt:

'Toetsen of het referentiemodel of conceptueel model – dat weergeeft hoe botnetbestrijding door Internet Service Providers technisch, organisatorisch en juridisch wordt aangepakt – overeenkomt met de wijze hoe Internet Service Providers botnetbestrijding in Nederland aanpakken.'

2.1.2 Hoofdvraag

Vanuit de hoofddoelstelling volgt de hoofdvraag van het afstudeeronderzoek:

'Welke rol spelen Internet Service Providers bij de bestrijding van botnets op het technisch gebied, hoe pakken ze dit organisatorisch aan en wat zijn juridisch gezien de mogelijkheden en beperkingen?'

2.2 Onderzoeksvragen

Om de hoofdvraag te kunnen beantwoorden, is er een aantal onderzoeksvragen opgesteld voor de theoretische fase en de empirische fase.

2.2.1 Vraagstelling theoretische fase (literatuuronderzoek)

Vanuit de doelstelling en het opgestelde onderzoeksmodel zijn de volgende onderzoeksvragen opgesteld:

- ***Wat zijn botnets?***
  In deze onderzoeksvraag wordt er in de literatuur gezocht naar een eenduidige definitie voor botnets. Daarnaast wordt er gekeken naar de eigenschappen van een botnet. De uitwerking van deze onderzoeksvraag is opgenomen in paragraaf 3.1.

- ***Hoe hebben botnets zich de afgelopen jaren geëvolueerd/ontwikkeld en welke gevolgen heeft dit?***
  Het is bekend dat botnets zich de afgelopen jaren hebben geëvolueerd/ doorontwikkeld. In deze onderzoeksvraag worden de in de literatuur beschreven doorontwikkeling van botnets weergegeven. Met deze onderzoeksvraag wordt er geprobeerd inzicht te geven in hoe botnets zich hebben geëvolueerd en hoe "lastig" het is, voor de organisaties die ze bestrijden, om dit bij te houden. De uitwerking van deze onderzoeksvraag komt terug in paragraaf 3.2.

- ***Hoe vindt de bestrijding van botnets plaats vanuit:***
  - ***technisch oogpunt***
  - ***organisatorisch oogpunt***
  - ***juridisch oogpunt?***

  In deze onderzoeksvraag wordt er dieper ingegaan op de literatuur waarin de bestrijding van botnets vanuit verschillende invalshoeken wordt beschreven. De uitwerking van deze onderzoeksvraag is opgenomen in paragraaf 3.3.

- ***Wat kunnen Internet Service Providers bijdragen in de bestrijding van botnets?***
  In deze onderzoeksvraag wordt door middel van de literatuur inzicht gegeven wat Internet Service Providers kunnen bijdragen aan de bestrijding van botnets. De uitwerking van deze onderzoeksvraag is opgenomen in paragraaf 3.4

- ***Welke juridische verantwoordelijkheden (rechten en plichten) hebben Internet Service Providers in relatie tot botnetbestrijding?***
  - ***Wat zijn ISP's wettelijk verplicht te doen aan botnetbestrijding?***

- ***Hoe ver gaan ISP's in botnetbestrijding?***

  Door middel van deze onderzoeksvraag wordt er geprobeerd vanuit de literatuur inzicht te krijgen in welke juridische verantwoordelijkheden ISP's hebben in relatie tot botnetbestrijding. De uitwerking van bovenstaande onderzoeksvraag is opgenomen in paragraaf 3.5.

- ***Wat doen Internet Service Providers afzonderlijk van elkaar aan botnetbestrijding?***
  In deze onderzoeksvraag wordt er geprobeerd vanuit de literatuur te onderzoeken wat de verschillende ISP's afzonderlijk van elkaar aan botnetbestrijding doen. Dit is opgenomen in paragraaf 3.6.

- ***Welke samenwerkingsinitiatieven zijn er te vinden over hoe Internet Service Providers samenwerken met andere partijen met betrekking tot botnetbestrijding?***
  Welke samenwerkingsinitiatieven zijn er beschreven in de literatuur over hoe ISP's samenwerken met andere partijen in de strijd tegen botnets. Dit is opgenomen in paragraaf 3.7.

Vanuit de literatuurstudie is er een conceptueel model geformuleerd en vervolgens is er op basis van het conceptueel model en de literatuurstudie een referentiemodel opgesteld.
Het conceptueel model geeft weer hoe de (relevante) aspecten van het onderzoek met elkaar in relatie staan. Het bevat een verzameling kernbegrippen (variabelen) die verwijzen naar bepaalde verschijnselen uit de werkelijkheid en (meestal) een verzameling causale relaties waarmee de veronderstelde verbanden tussen de kernbegrippen is vastgelegd. Het referentiemodel kan worden gezien als een concretisering van het conceptueel model.

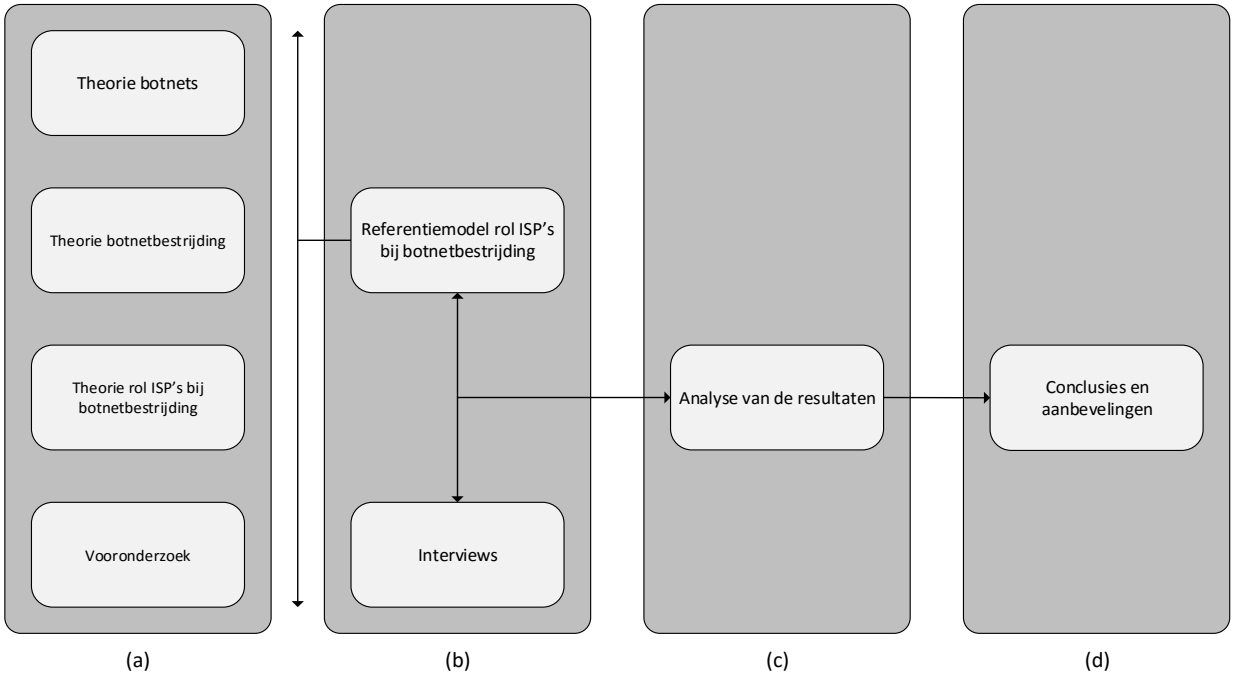
2.2.2 Vraagstelling Empirische fase

Vervolgens zijn vanuit de doelstelling voor de empirische fase de volgende onderzoeksvragen opgesteld:

- ***Wat wordt door ISP's verstaan onder botnets?***
- ***Hoe worden botnets geclassificeerd door ISP's?***
- ***Aan welke samenwerkingsverbanden worden door ISP's deelgenomen (op nationaal, Europees en wereldwijd niveau)?***
- ***Is het opgestelde theoretisch referentiemodel compleet?***
  Zijn er aspecten op het gebied van botnetbestrijding die niet voorkomen in het theoretisch referentiemodel, maar wel van toepassing zijn op de manier waarop botnetbestrijding wordt uitgevoerd door ISP's?
- ***Is het opgestelde theoretische referentiemodel correct?***
  Zijn de aspecten die voorkomen in het theoretisch referentiemodel van toepassing op het juiste gebied (technisch, organisatorisch, juridisch)?

2.3 Conceptueel onderzoeksmodel

Een onderzoeksmodel beschrijft globaal de structuur van een onderzoek, laat zien welke stappen worden doorlopen en geeft inzicht in de samenhang. In Figuur 2 is het onderzoeksmodel voor het onderzoekstraject opgenomen. Het figuur beschrijft de structuur van het onderzoek conform Verschuren en Doorewaard (2007).



Figuur 2 Onderzoeksmodel

Het onderzoeksmodel uit Figuur 2 kan als volgt worden verklaard:

> *Een bestudering van de recente en relevante theorie op het gebied van botnet, botnetbestrijding en de rol van ISP's bij botnetbestrijding, het doornemen van relevante ontwikkelingen in de strijd tegen botnets, het doen van een vooronderzoek door de raadpleging van experts en het volgen en bijwonen van congressen en seminars (a) levert als resultaat een referentiemodel (b) op dat geëvalueerd gaat worden door semigestructureerde interviews met deskundigen. Vervolgens zal er een vergelijkende analyse (c) worden gemaakt, die vervolgens resulteert in conclusies en aanbevelingen (d) voor vervolgonderzoek op het gebied van botnetbestrijding door ISP's.*

2.4 Soort onderzoek

Door Saunders (2011) worden vier verschillende soorten onderzoek onderscheiden: beschrijvend onderzoek, verkennend onderzoek, verklarend onderzoek en projecterend onderzoek.

Het uitgevoerde onderzoek is verkennend van aard. Een verkennend onderzoek is meestal kwalitatief van aard en levert ongestructureerde informatie op. Volgens Saunders (2011) zijn er drie belangrijke manieren om een verkennend onderzoek uit te voeren namelijk:

- Literatuuronderzoek;
- Praten met experts op het desbetreffende gebied;

- Het houden van een focusinterview.

2.5 Methode van onderzoek voor het theoretisch deel

Het theoretische deel is uitgevoerd door middel van een literatuuronderzoek. In dit afstudeeronderzoek heeft de literatuurstudie het doel om antwoord te geven op de onderzoeksvragen, waardoor er inzicht wordt verkregen in de huidige theorie met betrekking tot botnetbestrijding. Daarnaast levert de literatuurstudie als resultaat het (theoretische) referentiemodel. Voor het uitvoeren van de literatuurstudie is de opgezet gevolgd zoals deze door Saunders et al. (2011) wordt beschreven.

2.5.1 Zoekstrategie

Bij de start van de literatuurstudie is er een verkenning van de literatuur uitgevoerd. De eerste verkenning in de literatuur leverde veel resultaten op, voornamelijk resultaten met betrekking tot theoretische achtergronden van botnets en de bestrijding van botnets. Wat opvallend was in de eerste verkenning is dat in meerdere onderzoeken de ISP's een belangrijke rol/positie toegedicht krijgen, maar dat dit nauwelijks verder is onderzocht.

In Tabel 3 is een opsomming opgenomen van zoektermen waarmee de eerste verkenning is uitgevoerd.

Tabel 3 Zoektermen

Zoekterm
Botnet
Evolution botnet
Botnet mitigation ISP
Role ISP botnet mitigation
Botnet mitigation collaboration
Internet Service Providers malware

Voor de eerste verkenning is voornamelijk gebruik gemaakt van de online search engine Google Scholar.

Na de eerste verkenning is het literatuuronderzoek uitgevoerd met behulp van de volgende twee zoekmethoden:

- zoektermen
- sneeuwbalprincipe

Door het sneeuwbalprincipe toe te passen, wordt er geprobeerd om literatuur te verkrijgen waar andere onderzoekers naar verwijzen. Dit wordt gedaan door in eerste instantie verwijzingen na te gaan in eerder gevonden artikelen. Een resultaat van het toepassen van de sneeuwbalmethode is bijvoorbeeld het artikel van Cooke genaamd 'The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets' (Cooke, Jahanian, & McPherson, 2005).

De gevonden publicaties zijn verwerkt in EndNote. Deze publicaties zijn beoordeeld op bruikbaarheid door aan alle publicaties een score toe te kennen. Deze score wordt bepaald op

basis van de samenvatting en de conclusie van de publicatie en daarnaast is er bij met name oudere publicaties gekeken naar het aantal keren dat een publicatie is geciteerd door andere onderzoekers.

2.5.2 Geraadpleegde bronnen

Voor het zoeken naar relevante literatuur is er gebruik gemaakt van online beschikbare wetenschappelijke databases. In deze online databases zijn tijdschriftartikelen, afstudeerrapporten en andere wetenschappelijke artikelen te vinden. Via de digitale bibliotheek van de Open Universiteit is er een lijst met digitale bronnen. Van deze lijst is een aantal digitale bronnen interessant met betrekking tot het afstudeeronderzoek. Deze zogenaamde digitale bronnen geven vaak toegang tot de full tekst artikelen. Voornamelijk zijn onderstaande digitale bronnen (zoekengines) gebruikt:

- Google scholar / Google Wetenschap
- IEEE
- ACM
- Springer
- Science Direct (Elsevier)

2.5.3 Wetenschappelijke validiteit bronnen

Gevonden bronnen zijn beoordeeld op basis van de samenvatting (abstract), indices van het artikel en de gevonden trefwoorden in het artikel. Verder is de bron beoordeeld op wetenschappelijk niveau. Hiervoor is gebruik gemaakt van de richtlijnen die zijn vermeld in de Blackboard course B9232B (afstudeertraject Business Process Management and IT) van de Open Universiteit.

Hieronder is een opsomming gegeven van punten die gebruikt zijn om de validiteit te beoordelen:

- de literatuurbron is gepubliceerd
- de literatuurbron is naspeurbaar (door iedereen terug te vinden)
- de literatuurbron is refereed volgens een betrouwbaar systeem (bijvoorbeeld peer, anoniem)
- de literatuurbron is gepubliceerd in journal of conference proceedings

2.5.4 Tussenresultaten en tussenconclusies

Tijdens het analyseren en zoeken naar literatuur werd er geconstateerd dat er voor het beantwoorden van de onderzoeksvragen veel literatuur gevonden kan worden over de volgende onderwerpen:

- theorie achter botnets;
- ontwikkeling van botnets;
- botnet bestrijding;
- samenwerkingsverbanden inzake botnetbestrijding;
- het belang van ISP’s bij botnetbestrijding.

De uitdaging ontstond bij het zoeken naar publicaties over de resultaten van de samenwerkingsverbanden van ISP's in het bestrijden van botnets. Hierover is weinig terug te vinden in de wetenschappelijke literatuur. Hetzelfde geldt ook voor het beantwoorden van de onderzoeksvraag over wat ISP's wel en niet mogen vanuit technisch, organisatorisch en juridisch oogpunt.

Er zijn publicaties gevonden over samenwerkingsverbanden van ISP's. Deze zijn echter niet wetenschappelijk. Er is wel vakliteratuur beschikbaar. In dit onderzoek zal deze vakliteratuur gebruikt gaan worden om de actuele stand van zaken weer te geven.

2.6 Methode van onderzoek van het empirisch deel

In deze paragraaf wordt het technisch onderzoeksontwerp voor het empirisch deel van het onderzoek in detail beschreven. Deze paragraaf beschrijft de volgende zaken: de gebruikte onderzoeksstrategie, de manier van gegevensverzameling, de betrouwbaarheid, methoden van analyse en een vooruitblik op de resultaten.

Zoals in paragraaf 2.4 beschreven, is dit een verkennend onderzoek. Met een verkennend onderzoek ben je wendbaar op het moment dat er nieuwe inzichten ontstaan (Saunders et al., 2011).

Voor het uit te voeren empirisch onderzoek dient er een keuze gemaakt te worden uit verschillende onderzoeksmethoden. Door Saunders et al. (2011) wordt een aantal onderzoeksmethoden gepresenteerd:

- Het experiment
- De enquête
- De casestudy
- Action research
- Grounded theory
- Etnografie
- Archiefonderzoek

Om tot een juiste keuze te komen in de te kiezen onderzoekstrategie voor het empirisch deel is een aantal afwegingen gemaakt. In Tabel 4 is per onderzoekstrategie een omschrijving gegeven.

Tabel 4 Overzicht onderzoeksmethoden

Onderzoeksmethode	Omschrijving
Experiment	Volgens Verschuren en Doorewaard (2007) is een experiment het type onderzoek waarmee ervaringen kunnen worden opgedaan met nieuwe te creëren situaties en processen en waarmee kan worden nagegaan wat de effecten zijn van de veranderingen.
Enquête	Enquête wordt geassocieerd met de deductieve methode. De enquête wordt ingezet als er is besloten om gestructureerd te interviewen. Het is een populaire en algemene strategie in onderzoek in het bedrijfsleven en het management en wordt het

	meest gebruikt om 'wie, wat, waar en hoeveel'-vragen te beantwoorden (Saunders et al., 2011).
Casestudy	Robson (2002, p. 178) definieert een casestudy als 'een methode voor het doen van onderzoek die gebruik maakt van empirisch onderzoek van een bepaald hedendaags verschijnsel binnen de actuele context, waarbij van verschillende soorten bewijsmateriaal gebruik wordt gemaakt'.
Action research	Bij Action Research ligt de expliciete nadruk op actie, namelijk het bevorderen van veranderingen binnen het bedrijf. Het is daarom bijzonder geschikt voor 'hoe'-vragen. Daarnaast is degene die het onderzoek uitvoert betrokken bij deze actie voor verandering en het elders toepassen van opgedane kennis (Saunders et al., 2011).
Grounded theory	Grounded theory is het opbouwen van een theorie of model door een combinatie van inductie of deductie (Saunders et al., 2011).
Etnografie	Etnografie is een inductieve methode. De etnografie is afkomstig uit de antropologie. Het doel ervan is het beschrijven en verklaren van de maatschappelijke wereld waarin de onderzochte personen leven, op de manier zoals zij die zouden beschrijven en verklaren (Saunders et al., 2011).
Archiefonderzoek	In het archiefonderzoek zijn administratieve gegevens en documenten de voornaamste bron van gegevens (Saunders et al., 2011). Een archiefonderzoeksmethode maakt onderzoeksvragen mogelijk die gericht zijn op het verleden en de veranderingen in de loop van de tijd, of ze nu verkennend, beschrijvend of verklarend zijn.

In Tabel 5 is de verantwoording opgenomen voor de gekozen onderzoeksstrategie.

Tabel 5 Afweging onderzoeksmethode

Onderzoeksmethode	Afweging
Experiment	Een experiment is binnen dit onderzoek niet geschikt, omdat: Er is geen sprake van een laboratoriumexperiment.
Enquête	Een enquête is binnen dit onderzoek niet geschikt, omdat: Er is sprake van een kwalitatief onderzoek. Over het onderwerp is veel achtergrondinformatie nodig. Het is niet mogelijk om door te vragen (te verdiepen).
Casestudy	Een casestudy is binnen dit onderzoek geschikt, omdat: De empirische vragen hebben betrekking op 'waarom', 'wat' en 'hoe'.
Action research	Action research is binnen dit onderzoek niet geschikt, omdat: Het gaat niet om het bevorderen van veranderingen binnen een specifieke context.
Grounded theory	Grounded theory is binnen dit onderzoek niet geschikt, omdat:

	Er geen gedrag wordt voorspeld en geprobeerd wordt te verklaren. Dit is een inductieve onderzoeksmethode en in dit onderzoek wordt er gebruik gemaakt van een deductieve onderzoeksmethode.
Etnografie	Etnografie is niet geschikt, omdat: Dit een inductieve methode is. Daarnaast is participeren niet mogelijk.
Archiefonderzoek	Archiefonderzoek is niet geschikt in dit onderzoek, omdat: Het niet mogelijk is om de onderzoeksvragen te beantwoorden op basis van administratie gegevens.

Zoals hierboven is vermeld, wordt in dit onderzoek de keuze gemaakt om een casestudy uit te voeren. Door Robson (2002) wordt een casestudy gedefinieerd als een methode voor het doen van onderzoek die gebruik maakt van een empirisch onderzoek van een bepaald hedendaags verschijnsel binnen de actuele context, waarbij van verschillende soorten bewijsmateriaal gebruik wordt gemaakt. De casestudy is vooral interessant als je een goed begrip wilt krijgen van de context van het onderzoek en de processen die worden doorlopen (Morris & Wood, 1991).

Bovenstaande strategie is heel geschikt voor het geven van antwoorden op de vraag ‘waarom?’ en ook op de vragen ‘wat?’ en ‘hoe?’. Daarom wordt de casestudymethode vaak gebruikt in verklarend en verkennend onderzoek (Saunders et al., 2011).

Het onderzoek dat uitgevoerd is, is een verkennend onderzoek, ook wel exploratief onderzoek genoemd. Volgens Saunders et al. (2011) is dit een waardevolle methode om uit te vinden ‘wat er gebeurt’ om zodoende nieuwe inzicht te verkrijgen en de optredende verschijnselen in een nieuwe context te beoordelen. Verder wordt door Saunders et al. (2011) aangegeven dat je een verkennend onderzoek uitvoert als je nog geen duidelijke voorspelling kan doen, maar wel vermoedens hebt.

2.6.1 Onderzoekspopulatie

De onderzoekspopulatie voor dit afstudeeronderzoek bestaat uit ISP’s die binnen Nederland actief zijn. Daarnaast is het opgestelde theoretisch referentiemodel ook getoetst bij het NCSC, die in een coördinerende rol heeft als het gaat om botnetbestrijding.

2.6.2 Methoden en technieken van dataverzameling

In dit onderzoek wordt er voor gekozen om gebruik te maken van interviews. Met behulp van interviews is het mogelijke om valide en betrouwbare gegevens te verzamelen die van belang zijn voor de onderzoeksvragen en onderzoeksdoelstellingen.

Bij interviews kan onderscheid worden gemaakt tussen verschillende soorten. In Tabel 6 is een overzicht opgenomen van de verschillende soorten interviews met daarbij een omschrijving.

Tabel 6 Typen interview (Saunders et al., 2011)

Type interview	Omschrijving
Gestructureerde	Gebruik van gestandaardiseerde of een identieke verzameling interviewvragen. Geen ruimte voor discussie.
Semigestructureerde	Niet gestandaardiseerde vragen. De onderzoeker heeft een lijst met thema's en vragen die moeten worden behandeld. Tijdens het interview is er ruimte om vragen aan te passen en of weg te laten. Vrijheid voor discussie.
Ongestructureerde	Informeel van aard. Wordt gebruikt om een algemeen gebied nader te onderzoeken. Veel ruimte voor discussie.

In dit onderzoek is de keuze gemaakt voor semigestructureerde interviews. semigestructureerde interviews kunnen worden gebruikt in samenhang met een verkennend onderzoek (Saunders et al., 2011).

2.6.3 Semigestructureerde interviews

Tijdens het interview is er gebruikt gemaakt van vraagverwerkingslijst. Deze vraagverwerkingslijst kan worden gezien als leidraad voor het interview. Tijdens de interviews is waar nodig doorgevraagd en zijn er vragen aangepast. Hiervoor is gekozen om de doelstelling en onderzoeksvragen niet uit het oog te verliezen. In bijlage 3 is de informatie opgenomen die voorafgaand aan het interview naar de deelnemers is toegestuurd met daarin de vragen en het referentiemodel.

Van elk interview is een uitwerking gemaakt en deze is ter controle naar de betreffende deelnemer toegestuurd. De opmerkingen van de deelnemer zijn vervolgens verwerkt.

2.6.4 Benodigde data en databronnen

Voor het empirisch onderzoek was het de bedoeling om het theoretische referentiemodel, dat is ontstaan naar aanleiding van het literatuuronderzoek, te toetsen aan de werkelijkheid. Hiervoor is contact gelegd met verschillende ISP's die actief zijn binnen Nederland. Daarnaast is contact gelegd met het NCSC dat het aanspreekpunt binnen Nederland is op het gebied van ICT-dreigingen en cybersecurityincidenten.

De geselecteerde personen zijn telefonisch, per email en LinkedIn benaderd. In bijlage 1 is een voorbeeld uitnodigingsemail opgenomen die naar de contactpersonen van de verschillende ISP's is verstuurd. Na het eerste contact met de ISP's kwam al snel het verzoek om anoniem deel te nemen aan het onderzoek. De uitnodigingsemails zijn vervolgens daarop aangepast. In sommige gevallen was een ISP, die benaderd werd, lid van de vereniging Abuse Information Exchange en werd hieraan in de uitnodigingsemail kort gerefereerd. In totaal zijn er negen ISP's benaderd waarvan er vijf bereid waren om mee te werken. Daarnaast was het NCSC bereid mee te werken aan het onderzoek.

Voorafgaand aan het interview is middels een toestemmingsformulier toestemming gevraagd voor het interview. In bijlage 2 is dit formulier opgenomen.

2.6.5 Ethische kwesties

Zoals aangegeven door Saunders et al. (2011) is een aandachtspunt tijdens het onderzoek de omgang met ethische kwesties. Echter, de manier waarop het onderzoek wordt uitgevoerd, wordt geleid door de ethische code van de onderwijsinstelling.

Tijdens het eerste contact met de mogelijke interviewkandidaten kwam naar voren dat de wens bestond om het semigestructureerde interview anoniem te laten plaatsvinden. Door de ISP's werd aangegeven dat het belangrijk is om het interview anoniem te voeren, omdat de informatie concurrentiegevoelig kan zijn en deze informatie mogelijk voordeel kan opleveren voor exploitanten van botnets.

In het uitgevoerde onderzoek zijn vertrouwelijkheid en anonimiteit voorwaarden om toegang te krijgen tot de verschillende ISP's zoals door Saunders et al. (2011) wordt aangegeven.

Om de anonimiteit en vertrouwelijkheid te waarborgen is er in dit onderzoek voor gekozen om, als gerefereerd wordt naar een interview, te spreken over ISP1, ISP2 enz. Daarnaast zijn alle interviews geanonimiseerd. Dit betekent concreet het volgende:

- Geen informatie naar de individuele ISP's;
- Geen naam van de kandidaat;
- Geen functiebeschrijving van de kandidaat;
- Geen plaatsnaam;
- Geen specifieke verwijzing naar bijvoorbeeld producten van deze ISP's.

2.6.6 Validiteit en betrouwbaarheid

Voor het onderzoek is een casestudy uitgevoerd. Tijdens deze casestudy is er gebruik gemaakt van semigestructureerde interviews. Volgens Saunders et al. (2011) is het mogelijk om met semigestructureerde interviews een hogere mate van validiteit te krijgen door het zorgvuldig uitvoeren van het interview, vragen nader te kunnen toelichten, dieper op de antwoorden in te gaan en de onderwerpen vanuit verschillende invalshoeken te bespreken.

Tijdens de voorbereiding van de interviews is hier al rekening mee gehouden door de interviews volgens een bepaalde structuur in te delen. Vervolgens is de vragenlijst opgezet en binnen deze vragenlijst was er de mogelijkheid om sommige vragen te verdiepen en andere vragen over te slaan.

In dit afstudeeronderzoek wordt er gebruik gemaakt van semigestructureerde interviews. Hierdoor kan er twijfel ontstaan over de betrouwbaarheid. Betrouwbaarheid in relatie tot kwalitatief onderzoek heeft te maken de vraag of verschillende onderzoekers dezelfde resultaten krijgen bij herhaling van het onderzoek. De vrees over de betrouwbaarheid van dit soort interviews heeft ook met problemen van bias of vertekening te maken. Het is mogelijk dat er een interviewerbias of een respondentbias optreedt.

Geprobeerd is om interviewbias te voorkomen door tijdens de interviews geen meningen of eigen oordelen te geven. Tot slot is er gepoogd om respondentbias te voorkomen door de interviews anoniem te verwerken.

Om de betrouwbaarheid te verhogen is het belangrijk om de interviews zorgvuldig voor te bereiden. De betrouwbaarheid van een onderzoek zal toenemen als de respondenten eensluidende antwoorden geven op een interviewvraag. In onderhavig onderzoek is er door de respondenten merendeels eensluidend geantwoord. In een enkel geval was er geen sprake van een eensluidend antwoord. Een voorbeeld hiervan is de vraag over classificatie van botnets. Door sommige ISP's worden botnetbesmettingen niet geclassificeerd en door andere wel. Echter, dit heeft geen nadelig effect op de betrouwbaarheid.

Als we kijken naar de betrouwbaarheid is het volgens Marshall en Rossman (1999) niet noodzakelijkerwijs de bedoeling dat de afgeleide resultaten, die zijn verkregen door het gebruik van in dit geval semigestructureerde interviews, herhaalbaar zijn. Dit komt omdat ze de werkelijkheid ten tijde van het interview weerspiegelen. Marshall en Rossman (1999) nemen aan dat de omstandigheden waarin dit soort onderzoek wordt gedaan complex en dynamisch is.

2.6.7 Wijze van analyseren

Na het uitvoeren van de semigestructureerde interviews zijn de antwoorden geanalyseerd met behulp van een kwalitatieve analyse.

De antwoorden van de interviews zijn kwalitatief vergeleken met het referentiemodel uit de literatuurstudie. Analyse van deze gegevens hebben geleid tot conclusies en aanbevelingen over de rol van ISP's bij de bestrijding van botnets en een referentiemodel dat weergeeft hoe ISP's botnetbestrijding uitvoeren.

3 Botnetbestrijding door ISP's

Dit hoofdstuk bevat de resultaten van het uitgevoerde literatuuronderzoek. De resultaten van het empirisch onderzoek worden behandeld in hoofdstuk 5.

In meerdere onderzoeken wordt aangegeven dat botnets één van de grootste bedreigingen zijn op het internet (Rodríguez-Gómez, Maciá-Fernández, & García-Teodoro, 2013; Tiirmaa-Klaar, Gassen, Gerhards-Padilla, & Martini, 2013; van Eeten, Asghari, Bauer, & Tabatabaie, 2011). In het Cybersecuritybeeld van 2013 wordt aangegeven dat botnets de grootste cyberbedreiging vormen in Nederland (Nationaal Cyber Security Centrum, 2013). In het daarop volgende Cybersecuritybeeld van 2014 wordt aangegeven dat het gebruik van botnets winstgevender wordt voor de cybercriminelen en dat botnets steeds beter worden verhuld en verdedigd (Nationaal Cyber Security Centrum, 2014).

In meerdere wetenschappelijke publicaties wordt een belangrijke rol toegedicht aan ISP's bij het bestrijden van botnets. In dit hoofdstuk wordt daarom eerst ingegaan op de achtergronden en de 'continue' evolutie van botnets om vervolgens een overzicht te geven van wat kunnen ISP's technisch, organisatorisch en juridisch ondernemen tegen botnets. Tot slot wordt er nog gekeken welke samenwerkingsverbanden er inzake botnetbestrijding in de literatuur zijn vermeld.

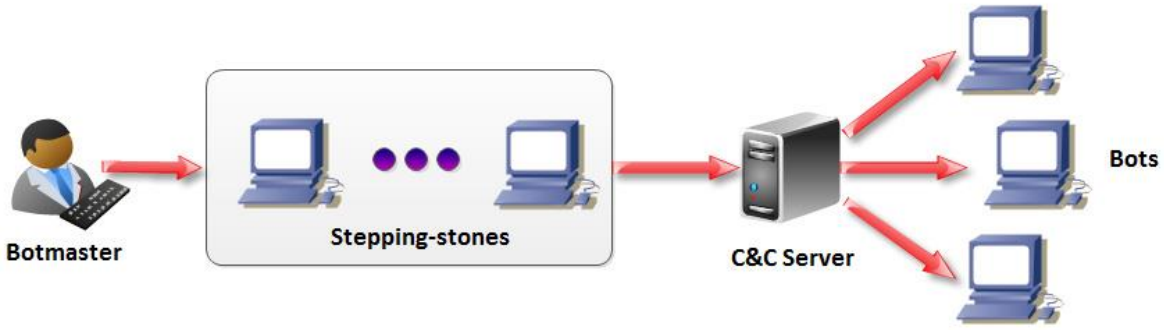
3.1 Botnets

In paragraaf 1.3 is al dieper ingegaan op wat een botnet is en daarnaast is er een definitie gepresenteerd voor een botnet die wordt gebruikt in dit onderzoek. In deze paragraaf wordt besproken wat een botnet is, hoe een botnet functioneert, hoe een botnet wordt aangestuurd en waarvoor een botnet kan worden gebruikt. De theoretisch onderzoeksvraag '***Wat zijn botnets?'*** kan worden beantwoord door de informatie vanuit paragraaf 1.3 samen met de in deze paragraaf gegeven informatie over botnets.

3.1.1 Onderdelen botnet

In Figuur 3 is de versimpelde structuur van een botnet weergegeven. In deze structuur is een aantal belangrijke zaken te herkennen, namelijk:

- Bot;
- Botmaster;
- Command and control;
- Botnet.



Figuur 3 Versimpelde structuur van een botnet (Khattak, Ramay, Khan, Syed, & Khayam, 2014)

3.1.2 Infectie en verspreiding mechanismen

Eén van de belangrijkste doelen van een botnet is het continue vergroten van zijn zogenaamde 'footprint' (groeien in aantal bots). De meeste bot binaries hebben ingebouwde mechanismen om zichzelf verder te kunnen verspreiden naar andere mogelijke hosts.

Het verspreidingsmechanisme van een botnet kan worden opgedeeld in actief en passief. Er wordt gesproken over actieve verspreiding als een botnet in staat is om zelf andere hosts te infecteren zonder menselijke tussenkomst. Een voorbeeld hiervan is dat een bot een netwerk scant op zoek naar nieuwe slachtoffers.

Bij passieve verspreiding heeft een gebruiker een bepaalde rol. Hieronder worden de drie meest gebruikte passieve technieken weergegeven die een botnet kan gebruiken voor verspreiding (Khattak et al., 2014; Li, Jiang, & Zou, 2009):

1. Drive-by Download
2. Infected media
3. Social Engineering

3.1.3 Doel van botnets

Botnets worden voor een diversiteit aan criminele activiteiten ingezet (Kim, Jeong, Kim, & So, 2010; Li et al., 2009; Plohmann, Gerhards-Padilla, & Leder, 2011; Silva et al., 2013; van Eeten, Lone, & Moura, 2014):

- Zoeken naar nieuwe machines die kunnen worden geïnfecteerd
- Versturen van spam
- DDoS (Denial of service attack) aanvallen
- Phishing
- Stelen van gevoelige data
- Identiteitsdiefstal
- Klik fraude
- Cyber warfare
- Cyber sabotage
- Verspreiden van andere malware
- Afpersing
- Manipuleren van online games

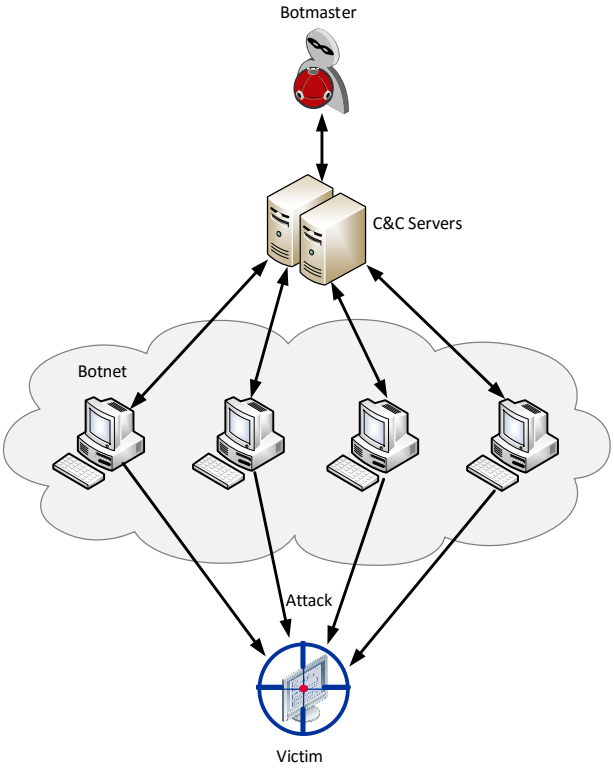
- Bitcoinmining

3.1.4 Aansturing van botnets

De manier/wijze hoe een botnet wordt aangestuurd is bepalend voor de organisatie van het botnet. In de literatuur zijn verschillende commandostructuren terug te vinden om bots aan te sturen.

3.1.4.1 Centrale commandostructuur

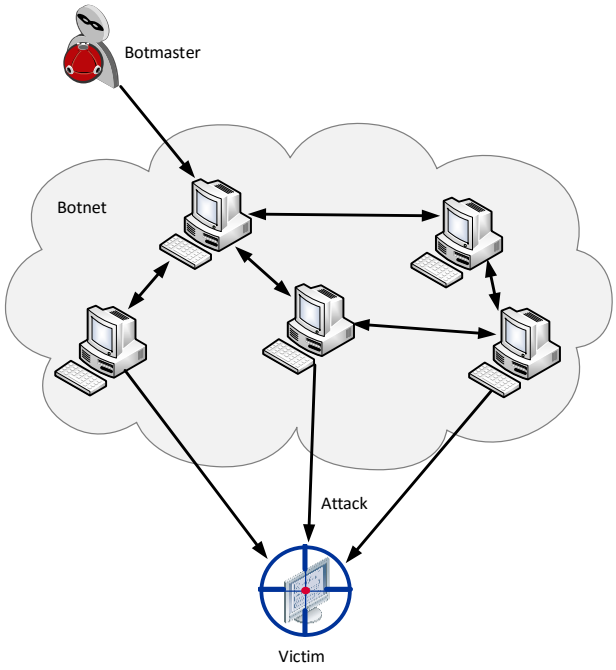
In de centrale commandostructuur wordt het veel gebruikte client-servermodel toegepast (Silva et al., 2013). De bot/zombiecomputer fungeert als cliënt en maakt verbinding met de server. Dit zijn gebruikelijke C&C servers. Deze C&C servers zijn verantwoordelijk voor het verzenden van commando's naar de bots en het verzorgen van malware updates. In Figuur 4 is een schematische weergave opgenomen van een centrale commandostructuur. In een centrale C&C structuur wordt vaak gebruik gemaakt van de IRC en http protocollen.



Figuur 4 Centrale commandostructuur

3.1.4.2 Decentrale commandostructuur

De decentrale commandostructuur maakt gebruik van P2P protocollen voor de botnet (Czosseck, Klein, & Leder, 2011). In deze structuur worden de commandolijnen onderling tussen de verschillende bots opgezet. De commando's worden door de bots onderling verspreid. In Figuur 5 is een versimpelde weergave opgenomen van een zogenaamde decentrale commandostructuur.

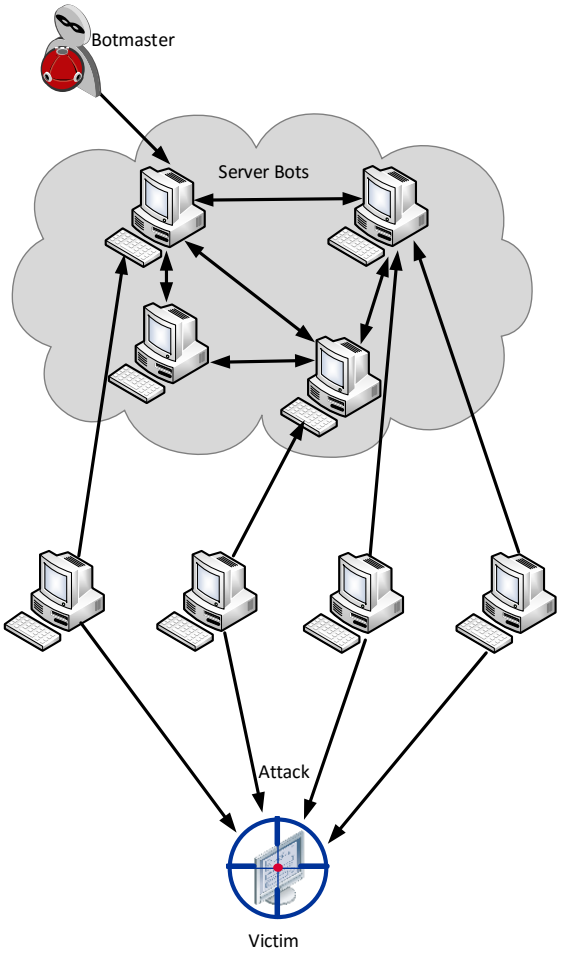


Figuur 5 Decentrale commandostructuur

In een onderzoek van Cooke et al. (2005) wordt de random commandostructuur gepresenteerd als een speciale variant op de decentrale structuur. Het idee achter de random commandostructuur is de volgende: een bot weet slechts over het bestaan van één andere bot (Banday, Qadri, & Shah, 2009). Hierdoor wordt de detectie van botnets veel moeilijker gemaakt. Vervolgens kan een botmaster willekeurig een bericht bij een bot achterlaten en deze bot kan vervolgens het bericht doorgeven aan slechts één andere bot. Deze commandostructuur heeft een hoge message latency en er is geen garantie dat een bericht wordt afgeleverd bij alle bots. Tot op heden is, voor zover bekend, deze structuur nog niet toegepast in de werkelijkheid (Banday et al., 2009).

3.1.4.3 Hybride model C&C

In een hybride botnet structuur worden de twee voorgaande structuren gebundeld (Rodríguez-Gómez et al., 2013). Een hybride structuur is dus een combinatie van de centrale en decentrale commandostructuur. In een hybride structuur worden technieken gecombineerd om met de sterke punten van één techniek de zwakke punten van de andere techniek te compenseren (Schless, 2013). In een hybride oplossing bestaan er één of meerdere gedistribueerde netwerken, elk met één of meer centrale servers (Rodríguez-Gómez et al., 2013). Een voorbeeld is dat een groep van bots zich kan gedragen als zogenaamde ‘servants’, omdat ze in staat zijn zich te gedragen als zowel cliënt en als server (OpenDNS, 2011; P. Wang, Sparks, & Zou, 2010). Hybride oplossingen kunnen P2P protocollen gebruiken op dezelfde wijze als in decentrale oplossingen. In Figuur 6 is een versimpelde weergave opgenomen van een zogenaamde decentrale commandostructuur.



Figuur 6 Hybride commandostructuur

3.1.5 Botnet communicatie

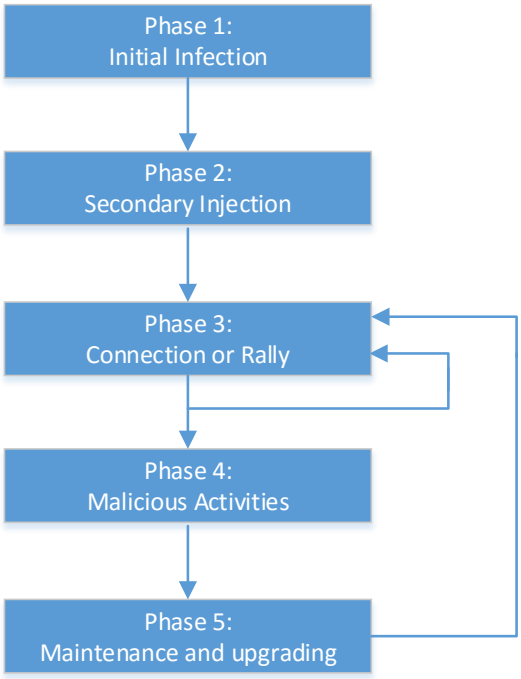
Als er een verbinding is tussen de bots en de C&C servers kunnen er verschillende communicatieprotocollen worden gebruikt, zoals bijvoorbeeld http of IRC.

Voor communicatie met de bot en voor de realisatie van de commandostructuur kunnen verschillende infrastructuren en protocollen worden gebruikt. De eerste botnets die werden ontwikkeld, maakten gebruik van het IRC protocol voor communicatie. Een ander protocol wat gebruik wordt, is het http protocol met normale GET en POST commando's.

3.1.6 Levenscyclus van een botnet

In verschillende artikelen wordt de levenscyclus voor een botnet weergegeven. De meeste artikelen kiezen er voor om de levenscyclus te beschrijven vanuit het oogpunt van de botmaster. De verschillende fasen worden soms aangegeven met verschillende namen, maar in het algemeen worden de verschillende fasen benoemd zoals in Figuur 7 is weergegeven (Silva et al., 2013). In de levenscyclus van een botnet zijn vijf verschillende fasen te benoemen (Feily, Shahrestani, & Ramadass, 2009). Als een machine eenmaal geïnfecteerd is, doorloopt hij een aantal fasen. Deze vijf fasen zijn hieronder weergegeven en beschreven:

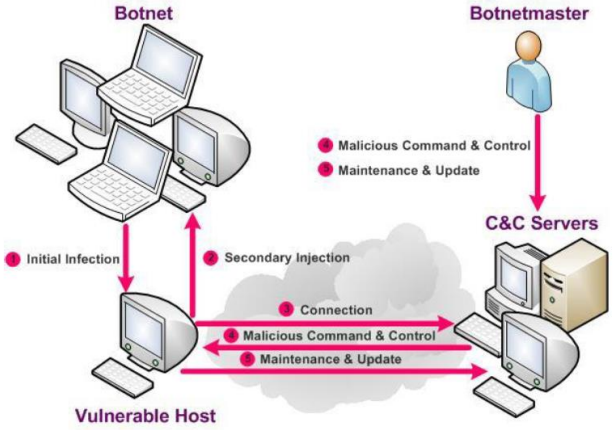
1. Initiële infectie fase – als een host is geïnfecteerd, wordt hij onderdeel van een potentiële bot. De infectie gebeurt meestal door een drive-by download, malware van een website, een email waarvan de bijlage is geïnfecteerd of via een besmette usb stick.
2. Secundaire infectie fase – als de eerste fase succesvol is, wordt deze fase gestart. In deze fase voert de geïnfecteerde host een programma uit dat zoekt naar de malware en dit wordt gedownload op de host.
3. Connectie fase – nu de malware is geïnstalleerd op de host kan er verbinding worden gemaakt met de C&C server om te kijken of er instructies/opdrachten zijn voor de host. De host hoeft niet continu online te zijn. De host kan bijvoorbeeld verbinding maken met de C&C server als de host wordt opgestart.
4. Malicious activities – in deze fase kan de geïnfecteerde machine worden ingezet voor kwaadaardige activiteiten zoals genoemd in paragraaf 3.1.3.
5. Update en onderhoudsfase – in deze fase kan de botsoftware worden geüpdatet. Door het updaten van de software kunnen er nieuwe features aan de bot worden toegevoegd, bijvoorbeeld om detectie te voorkomen. Ook is het mogelijk om de verwijzing naar bijvoorbeeld de C&C server te veranderen.



Figuur 7 Levenscyclus van een botnet (Feily et al., 2009; Silva et al., 2013)

In Figuur 8 wordt de levenscyclus van een botnet middels een illustratie weergegeven. Gedurende de initiële fase (initial phase) scant de aanvaller zijn doel op bekende kwetsbaarheden en infecteert de botmaster zijn doelwit via verschillende exploitmethodes. Na de initiële infectie volgt de secundaire injectiefase. In deze fase voert de geïnfecteerde machine een script uit (shell-code). Vervolgens wordt in deze fase een uitvoerbaar bestand binnen gehaald en geïnstalleerd op het doelwit. Op het moment dat de installatie succesvol is, verandert de machine in een zogenaamde zombie. In de connectiefase legt de bot een verbinding met zijn 'command and control' server. In deze fase wordt de machine onderdeel van het botnet. In de volgende fase kan de bot worden gebruikt voor zogenaamde malicious activiteiten. De bot is in staat om commando's/opdrachten te ontvangen. De update- en

onderhoudsfase is er op gericht om de bot te onderhouden en up te daten. Er kan in deze fase een update worden geïnstalleerd van de botsoftware met nieuwe mogelijkheden.



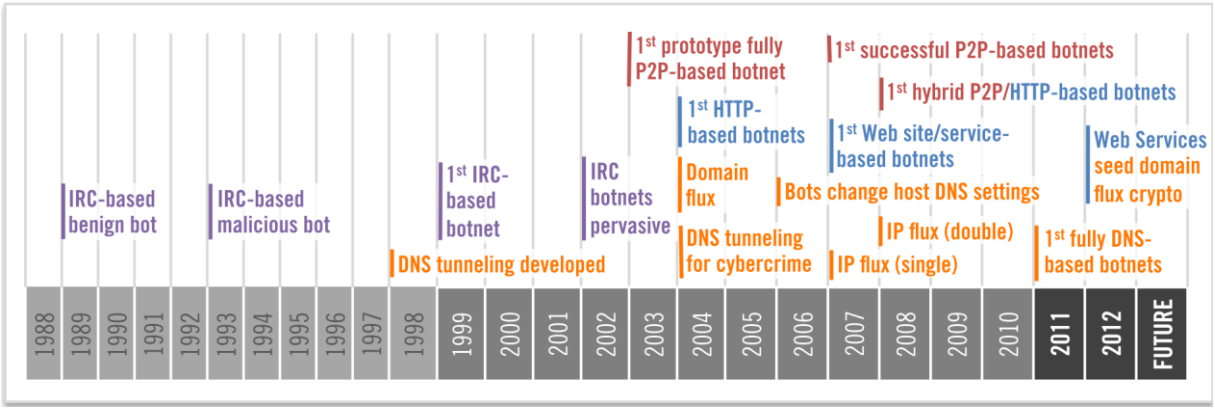
Figuur 8 Levenscyclus van een botnet (Feily, et al. 2009)

3.2 Evolutie botnets

In deze paragraaf wordt een overzicht gegeven van de evolutie van botnets. Hiermee wordt de onderzoeksvraag '***Hoe hebben botnets zich de afgelopen jaren geëvolueerd/ontwikkeld en welke gevolgen heeft dit?'*** beantwoord.

In meerdere wetenschappelijke artikelen wordt een overzicht gegeven van de evolutie/doorontwikkeling van botnets (Li et al., 2009; Silva et al., 2013).

In Figuur 9 wordt de evolutie van botnets weergegeven (OpenDNS, 2011). De eerste botnets (vanaf 1989) maakten gebruik van een centrale commandostructuur, maar deze structuur was erg kwetsbaar (Grizzard, Sharma, Nunnery, Kang, & Dagon, 2007). Rond 2002 werden de eerste decentrale botnets ontdekt die gebruik maakten van peer-to-peer. Tegenwoordig worden er botnets ontdekt die hybride kenmerken in zich hebben. In meerdere studies wordt gemeld dat in een groot deel van botnets, die vandaag de dag worden ontdekt, gebruik wordt gemaakt van een decentrale structuur.



Figuur 9 Evolutie botnets (OpenDNS, 2011)

Daarnaast heeft het ontwikkelen van botnets zich sinds 2004 verplaatst van achterkamertjes naar criminele organisaties en worden botnets nu soms zelfs door overheden ingezet (Zetter,

2014). Tot 2004 waren er voornamelijk amateur hackers actief, maar sinds 2004 is online crime steeds meer een serieuze bedrijfstak geworden (Moore et al., 2009).

Als we kijken naar de evolutie van botnets is ook de wijze van infectie en verspreiding van botnets geëvolueerd. Volgens Shin, Lin, en Gu (2011) zijn er twee infectietechnieken te benoemen, namelijk:

- Bots die zichzelf verspreiden/voortplanten (auto-self-propagating, Type I).
  In dit geval maken de bots gebruik van network scanning technieken om zo kwetsbare hosts te vinden en deze te infecteren door bijvoorbeeld gebruik te maken van een exploit. Deze aanpak is actief en agressief in het infecteren van machines.
- Bots die zichzelf verspreiden met de hulp van mensen of via andere methoden (non-self-propagating, Type II).

Doordat botnets evolueren, neemt de diversiteit toe (T. Wang, Wang, Liu, & Shi, 2013). Om botnets te bestrijden, is indeling in groepen daarom belangrijk. In meerdere studies is er voor gekozen om botnets in te delen aan de hand van de commandostructuur. Door T. Wang et al. (2013) wordt voorgesteld om botnets in te delen aan de hand van het gebruikte patroon. Het voordeel hiervan is dat botnets, die gebruik maken van meerdere lagen, kunnen worden onderscheiden van 'gewone' botnets. Een voorbeeld hiervan is de Conficker botnet. Daarnaast wordt door T. Wang et al. (2013) aangegeven dat botnets middels deze nieuwe indeling beter kunnen worden onderzocht en bestreden.

In meerdere artikelen wordt er gerefereerd aan het feit dat er een zogenaamd kat en muis spel gaande is tussen botnet ontwikkelaars/operators en de security experten (Czosseck et al., 2011). Op dit moment voeren de cybercriminelen/botnetontwikkelaars de boventoon.

3.3 Bestrijding botnets

In de paragraaf 3.1 is dieper ingegaan op wat is een botnet. In deze paragraaf wordt dieper ingegaan op de bestrijding van botnets vanuit een technisch-, organisatorisch- en juridisch oogpunt. Hiermee wordt de onderzoeksvraag '***Hoe vindt de bestrijding van botnets plaats vanuit: technisch oogpunt, organisatorisch oogpunt en juridisch oogpunt'*** beantwoord.

In het artikel Botnets: Detection, Measurement, Disinfection & Defence (Plohmann et al., 2011) wordt een overzicht gegeven van de verschillende stappen die bij botnetbestrijding worden doorlopen. In Figuur 10 is het versimpelde proces opgenomen van botnetbestrijding. Het gevecht tegen een botnet begint met detectie van een botnet, daarna het bepalen van de eigenschappen van het botnet en tot slot de tegenmaatregelen die genomen kunnen worden. Vaak wordt detectie en het bepalen van de eigenschappen van een botnet als één stap in het botnetbestrijdingsproces gezien.

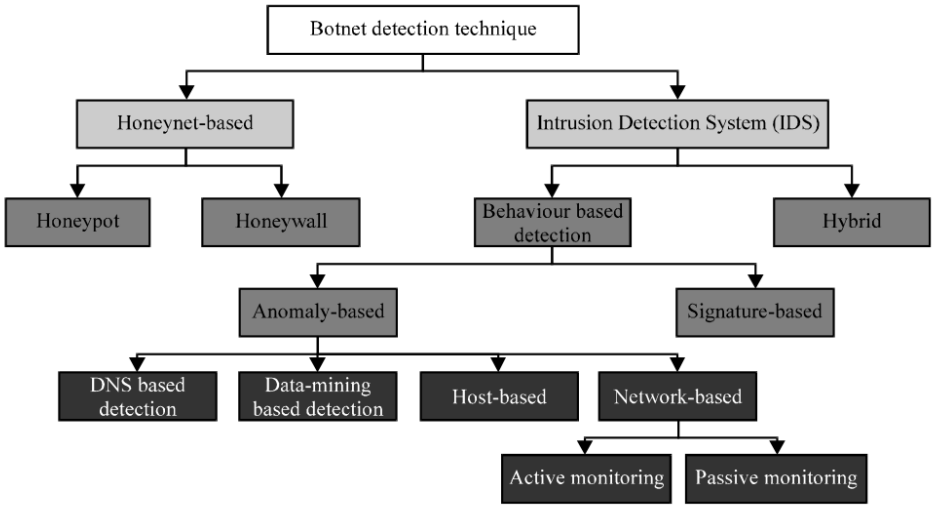
Figuur 10 Proces botnetbestrijding

3.3.1 Botnetdetectie

Het detecteren van botnets kan worden ingedeeld in twee verschillende manieren, namelijk (Abdullah, Abu, Faizal, & Noh, 2014):

- Honeynet-based;
- Intrusion Detection System (IDS)

In Figuur 11 is een totaal overzicht opgenomen met de verschillende botnet detectietechnieken (Abdullah et al., 2014). In Figuur 11 worden de botnet detectietechnieken onderverdeeld in Honeynet-based en Intrusion Detection System-based. Honeynets zijn van belang om de eigenschappen van botnets te leren kennen en de technieken die worden gebruikt te onderscheiden (Feily et al., 2009). Een Intrusion Detection Systems (IDS) kijkt naar bekende botnet signatures of afwijkingen in het netwerkverkeer. Door Silva et al. (2013) wordt een IDS onderverdeeld in signature- of anomaly-based. In het onderzoek van Abdullah et al. (2014) wordt nog een extra groep toegevoegd, namelijk hybrid-based.



Figuur 11 Botnet detection technique (Abdullah et al., 2014)

3.3.2 Countermeasures/tegenmaatregelen

Nadat een botnet is gedetecteerd, is het mogelijk om tegenmaatregelen te nemen en zodoende het botnet te bestrijden. Deze tegenmaatregelen kunnen zowel technisch, organisatorisch en juridisch van aard zijn.

Een traditionele manier om actie te ondernemen tegen een botnet is om de zwakke plek te vinden in zijn infrastructuur waardoor de botnet kan worden gemanipuleerd, onderbroken of kan worden geblokkeerd. Vaak wordt er samengewerkt met een ISP om toegang te krijgen tot het centrale punt van een botnet om het botnet op deze manier te onderbreken (Leder, Werner, & Martini, 2008).

Acties om een botnet uit te schakelen of de werking te verzwakken, kunnen zich richten tegen de verschillende onderdelen van een botnet (individuele bots, de structuur of de commandokanalen) (Estrada & Nakao, 2010; Schless, 2013). Zoals door Schless (2013) wordt aangegeven is het haast onmogelijk om alle individuele bots uit een botnet op te sporen.

Door Czosseck et al. (2011) en Leder, Werner, en Martini (2009) worden dit de klassieke tegenmaatregelen genoemd. Door Schless (2013) wordt er een tabel gepresenteerd met daarin per aangrijpingspunt de methode om een botnet te bestrijden. In Tabel 7 is deze in aangepaste vorm opgenomen.

Tabel 7 Botnetbestrijdingsmethoden gebaseerd op Schless (2013)

Aangrijpingspunt	Methode
Bot	Verwijderen bots uit het botnet (op een eigen netwerk).
Botnetstructuur	Overname of uitschakelen commandoserver(s)
	Verstoring van het botnet met gemanipuleerde bots (zelfvernietigingsopdracht, vervuiling van gegevens).
	Overname of verstoring van het botnet door manipulatie van de communicatie (zelfvernietigingsopdracht, vervuiling van gegevens, opdrachten van botmaster afvangen, blokkeren van domeinnamen en IP-adressen).
Botmaster(s)	Arresteren en vervolgen van de botmaster(s).
	Botmaster(s) en/of opdrachtgevers en/of infrastructuur fysiek uitschakelen.

3.3.3 Botnetbestrijding vanuit een technisch oogpunt

Door Plohmann et al. (2011) wordt een lijst gegeven van technische maatregelen die kunnen worden genomen tegen een botnet. Deze lijst is opgenomen in Tabel 8.

Tabel 8 Technische countermeasures (Plohmann et al., 2011)

Countermeasure
Blacklisting
Distribution of fake credential's
BGP Blackholing
DNS-based countermeasures
Direct Takedown of C&C Server
Packet filtering on Network and Application Level
Port 25 Blocking
Walled Gardens
Peer-to-Peer counter measures
Infiltration and Remote Disinfection

Bij sommige technische maatregelen, die kunnen worden genomen, zijn wel juridische beperkingen op te merken, zoals bijvoorbeeld infiltration.

3.3.4 Botnetbestrijding vanuit een organisatorisch oogpunt

Een botnet richt zicht met zijn acties niet vaak tot een individueel land. Cybercriminaliteit is vaak wereldwijd. De tegenmaatregelen kunnen alleen maar effectief zijn als ze op wereldwijd niveau worden uitgevoerd. In de studie van Leder et al. (2009) wordt aangegeven dat 'countermeasures' alleen effectief kunnen zijn als ze op wereldwijde schaal worden uitgevoerd.

Als er gekeken wordt naar hoe botnetbestrijding vanuit een organisatorisch oogpunt plaatsvindt, valt het volgende op. Om een botnet te bestrijden of zijn werking te verstoren, zijn er meerdere organisaties betrokken. Door het Nationaal Cyber Security Centrum (2013) wordt aangegeven dat onderzoek, infiltratie en sabotage van botnets in de praktijk vaak wordt uitgevoerd door private partijen. Onderzoeksinstellingen en securitybedrijven kunnen vrijer opereren dan de overheid die gehouden is aan allerlei regelgeving.

Op 25 februari 2015 werd door Cybercrime Centre van Europol melding gemaakt van het neerhalen van een botnet door een samenwerking van publieke en private partijen (Europol, 2015). In deze specifieke case ging het om een botnet genaamd Ramnit die 3,2 miljoen computers wereldwijd heeft geïnfecteerd. In het persbericht worden verschillende partijen genoemd die betrokken zijn bij het neerhalen van deze specifieke botnet. Het volgende valt op: de partijen die betrokken zijn bij het neerhalen van deze botnet werken vanuit verschillende landen binnen Europa. Ook valt op dat het in deze Europese samenwerking gaat om publieke en private partijen.

In verschillende studies wordt vermeld dat botnetbestrijding vaak grensoverschrijdend is. Zo wordt in 'Botnets: A survey' het volgende gesteld (Silva et al., 2013):
"Botnets are widespread in a distributed environment, so each botnet may involve several countries. Botnet activity could be legally restrained according to a specific local law issued by a nation. Agreements between countries are thus needed to prosecute cyber-crime in a consistent and coordinated way. Steps should also be taken to raise awareness among political decision-makers about the severity of the botnet"

3.3.5 Botnetbestrijding vanuit een juridisch oogpunt

Om een zogenaamde takedown van een botnet uit te voeren, zijn vaak juridische beperkingen te verwachten. In sommige landen is het verboden of gecompliceerd om een botnet neer te halen (Czosseck et al., 2011).

In opdracht van SURFnet is er een expert opinion geschreven door Koops (2013). In deze expert opinion wordt het volgende aangegeven met betrekking tot een takedown van een botnet. De meeste anti-botnetacties maken inbreuk op de vertrouwelijkheid, integriteit, beschikbaarheid of computergegevens van anderen. Er wordt in de expert opinion aangegeven dat de meeste acties tegen botnets al snel kunnen worden gezien/gekwalificeerd als handelingen die in computercriminaliteitsbepalingen worden beschreven als aftappen en opnemen van communicatie, hacken, gegevensaantasting, computersabotage en heling van gegevens.

In 2013 is er door de minister van Veiligheid en Justitie begonnen met een conceptwetsvoorstel om de opsporing en vervolging van computercriminaliteit te verbeteren (Ministerie van Veiligheid en Justitie, 2013). Na aanpassing is deze zogenoemde 'terughackwet', wetsvoorstel computercriminaliteit III, begin 2015 opnieuw ingediend bij de Tweede Kamer. Deze wet moet het mogelijk maken om het zogenoemde terughacken te legaliseren.

Bij het nemen van maatregelen tegen botnets moet in de meeste gevallen rekening worden gehouden met lokale wetgeving. Voor het succesvol bestrijden van een botnet zijn twee belangrijke factoren te noemen, namelijk de organisatorische en politieke factor (Leder et al., 2009).

3.4 Botnetbestrijding door ISP's

In deze paragraaf wordt een overzicht gegeven wat ISP's kunnen bijdragen in de strijd tegen botnets. Hiermee wordt de onderzoeksvraag '***Wat kunnen Internet Service Providers bijdragen in de bestrijding van botnets?'*** beantwoord.

In de literatuur zijn verschillende studies te vinden die een centrale rol toedichten aan ISP's in de strijd tegen botnets.

Uit een studie van Eeten et al. (2010) blijkt dat het probleem van botnets niet voor elke ISP even groot is. Er zijn ISP's waar relatief veel botnet geïnfecteerde machines zijn en ISP's waar het aantal relatief laag ligt. In het onderzoek van van Eeten bleek dat er weinig empirische data beschikbaar is om te veronderstellen dat ISP's het centrale punt zijn in botnetbestrijding en dat grotere ISP's slechter presteren in botnetbestrijding dan kleine ISP's (van Eeten et al., 2010). van Eeten et al. (2014) komt in later onderzoek tot de conclusie, gebaseerd op empirische data, dat ISP's een centrale rol kunnen spelen in botnetbestrijding.

In het onderzoek van Schless (2013) wordt het volgende geschreven over de rol van internetaanbieders bij botnetbestrijding. Internetaanbieders moeten in ieder geval in staat zijn om botnets op hun netwerken te herkennen. Voor de bestrijding van botnets moet vaak ontcijfering van gegevens plaatsvinden, infiltratie en/of overname van botnets. Dit zijn zaken die als computervredebreuk kunnen worden beschouwd en dit is in Nederland strafbaar.

De mate waarin ISP's activiteiten ondernemen om botnets te detecteren in hun netwerk is niet of nauwelijks beschreven in de literatuur. Het is bijvoorbeeld niet duidelijk of ISP's systemen plaatsen in hun netwerk om bijvoorbeeld deep packet inspection uit te voeren.
Echter, uit de literatuur blijkt dat er allerlei samenwerkingsverbanden zijn om botnets te bestrijden. In paragraaf 3.7 wordt er dieper ingegaan op deze samenwerkingsverbanden. In sommige gevallen worden er door diverse samenwerkingsverbanden best practices gepubliceerd over hoe ISP's bij kunnen dragen in de strijd tegen botnets. In verschillende studies wordt er verwezen naar deze zogenaamde security practices. In de master scriptie van Asghari (2010) wordt een 'complete' lijst gepubliceerd en vervolgens wordt van al deze best practices door Asghari een totaal overzicht gepresenteerd.

In Tabel 9 staat een overzicht van publicaties zoals die Asghari (2010) is gebruikt om een set van verschillende security maatregelen op te stellen die werkelijk in gebruik zijn door de industrie.

Tabel 9 Overzicht gevonden best security practices (Asghari, 2010)

Publicatie
Provider Security Measures (ENISA 2007)
Best Practices in Anti-Spam (ETIS 2007; MAAWG 2005; Schryen 2007 ch. 4; Sendmail 2007; OECD 2005)
Best Practices in Anti-Phishing (MAAWG and APWG 2006)
Best Practices for Mitigating Bot Infections (MAAWG 2009, 2007a; Livingood et al. 2009)
General Best Practices for ISP's and Network Operators (MAAWG 2007b; IndustryCanada 2005)

Vanuit de verschillende best (security) practices kan een groot aantal maatregelen worden gehaald die door ISP's kunnen worden geïmplementeerd in de strijd tegen botnets. Door Asghari (2010) worden de maatregelen onderverdeeld in 9 hoofgroepen. Namelijk:

- Active abuse handling
- Proactive detection of malicious activity
- Filtering malicious traffic and content
- User education and awareness
- Client security and quarantining
- Using updated network protocols and servers
- Participation in the security community
- Management and administrative procedures
- Legal measures

In de studie van Asghari (2010) wordt vervolgens een tabel gepresenteerd met daarin per hoofdgroep (security) maatregelen die ISP's kunnen nemen. In bijlage 4 is dit overzicht opgenomen. Sinds het door Asghari (2010) gepubliceerde onderzoek is er nog een aantal nieuwe best practices gepubliceerd en een aantal reeds gepubliceerde best practices is vernieuwd. In Tabel 10 is een overzicht van nieuwe publicaties opgenomen. Deze lijst is samengesteld op basis van in de verschillende publicaties genoemde best practices.

Tabel 10 Lijst met recente security practices

Publicatie
U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISP's) (Online Trust Alliance, 2013)
Combatting Botnets Through User Notification Across the Ecosystem (Online Trust Alliance, 2012)
Botnet Remediation Overview & Practices (Online Trust Alliance, 2013)
Internet Service Provider (ISP) Network Protection Practices (CSRIC, 2010)
Recommendations for the Remediation of Bots in ISP Networks (Livingood & Mody, 2012)
Internet Service Providers Voluntary Code of Practice (Internet Industry Association, 2014)
M^{3}AAWG Best Common Practices for the Use of a Walled Garden (Messaging Malware and Mobile Anti-Abuse Working Group, 2015)

In een publicatie van de Online Trust Alliance wordt de anti-botnet life cycle gepresenteerd. In de anti-botnet life cycle wordt botnetbestrijding onderverdeeld in vijf hoofdgebieden. In Figuur 12 is de anti-botnet life cycle weergegeven.

Figuur 12 Anti-botnet life cycle (Online Trust Alliance, 2013)

De vijf gebieden waarin door de Online Trust Alliance botnetbestrijding is onderverdeeld:

- Preventie (prevention) - proactieve maatregelen/activiteiten vanuit de ISP om te voorkomen dat een device geïnfecteerd raakt.
- Detectie (detection) – maatregelen/activiteiten met als doel het identificeren van bedreigingen op het netwerk van bijvoorbeeld een ISP.
- Notificatie (notification) – maatregelen/activiteiten die worden ondernomen om gebruiker of verantwoordelijke te informeren.
- Verwijdering/bestrijding (remediation) – maatregelen/activiteiten die worden ondernomen om malware te verwijderen van een geïnfecteerd device.
- Herstel (recovery) – maatregelen/activiteiten die worden ondernomen om de impact van een aanval op te lossen.

De in de verschillende publicaties gevonden aanbevelingen/best practices, die ISP's kunnen toepassen in de strijd tegen botnets, zijn onderverdeeld in de verschillende gebieden en waar nodig samengevoegd.

3.4.1 Preventie

In Tabel 11 is een overzicht opgenomen van aspecten die ISP's kunnen toepassen ter preventie van botnets.

Tabel 11 Preventie

Aspect	Naam kenmerk	Omschrijving
P-1	Beschikbaar stellen end-point security	ISP's stellen end-point security oplossingen beschikbaar voor hun klanten. Dit kan bijvoorbeeld door klanten een antivirussoftware aan te bieden of een router met beveiliging.

P-2	Educatie van klanten	Door ISP's wordt er actief uitleg gegeven over het gevaar van botnets en de acties die klanten kunnen ondernemen om dit te voorkomen. Hierbij valt te denken aan: waarom klanten hun software up-to-date moeten houden, bewustwording campagnes, aanmoedigen van klanten om een end-point security oplossing te gebruiken, belang van backups en acties die klanten kunnen ondernemen om niet onderdeel te worden van een botnet. Eén van de doelen van educatie van klanten is de volgende: dat er bij de klant bewustwording ontstaat dat hij mede verantwoordelijk is in het voorkomen van een botnetbesmetting (gedeelde verantwoordelijkheid).
P-3	Delen/communiceren van informatie/procedures omtrent botnetbestrijding	Door ISP's wordt er actief gecommuniceerd met andere stakeholders over botnetbestrijding. Door ISP's wordt bijvoorbeeld informatie gedeeld met andere stakeholders over lessons-learned en procedures inzake botnetbestrijding.
P-4	Deelnemen in een samenwerkingsverband inzake botnetbestrijding	Door ISP's wordt actief deelgenomen in samenwerkingsverbanden met betrekking tot botnetbestrijding.
P-5	Intrusion Prevention Systems (IPS)	ISP's maken gebruik van Intrusion Prevention Systems (IPS) om botnetbesmettingen te kunnen voorkomen.
P-6	Nemen van technische maatregelen inzake botnets	ISP's kunnen een aantal technische maatregelen nemen zodat het moeilijker wordt voor een botnet om machines te infecteren. Bijvoorbeeld het beveiligen van DNS servers.
P-7	Bijhouden stand van zaken met betrekking tot botnet/malware technieken.	ISP's blijven op de hoogte van de laatste ontwikkelingen met betrekking tot botnets en malware. Bijvoorbeeld door het trainen van personeel met betrekking tot bestrijding en detectie van botnets.
P-8	Klant support processen	Door de ISP's zijn er processen ingericht omtrent klantondersteuning inzake botnetbesmettingen.
P-9	Abuse team	ISP's hebben een abuse team actief.
P-10	Service Level Agreements	ISP's richten Service Level Agreements in met betrekking tot botnetbestrijding.
P-11	Standaardisering	Voldoen aan internationale standaarden inzake beveiliging (ISO 27002:2005, ISO 27006:2007)

3.4.2 Detectie

In Tabel 12is een overzicht opgenomen van aspecten die ISP's kunnen toepassen ter detectie van botnets.

Tabel 12 Detectie

Aspect	Naam kenmerk	Omschrijving
D-1	Aanbieden self-identify portal	Gebruikers zelf via tools, web portal of andere resource een mogelijke infectie laten vaststellen

D-2	Ontvangen informatie over mogelijke besmettingen via klanten	ISP's kunnen van klanten informatie krijgen over besmettingen binnen hun netwerk.
D-3	Communiceren gedetecteerde besmettingen	ISP's delen informatie over gedetecteerde besmettingen met andere ISP's.
D-4	Ontvangen informatie over mogelijke besmettingen via externe partijen	ISP's kunnen informatie over kwaadaardige activiteiten en bot geïnfecteerde klanten krijgen van externe partijen.
D-5	Ontvangen informatie over mogelijke besmettingen via AbuseHUB	ISP's ontvangen informatie over mogelijke besmettingen vanuit het AbuseHUB systeem.
D-6	Honeynet	ISP's maken gebruik van honeypots om besmettingen in het netwerk te kunnen constateren.
D-7	Detectie besmetting	Als een besmetting wordt geconstateerd, of daarop wordt gewezen door een derde, zal de ISP binnen een redelijke termijn beoordelen of hij hier tegen moet optreden.
D-8	Intrusion Detection Systems (IDS)	ISP's maken gebruik van Intrusion Detection Systems (IDS) om botnetbesmettingen te kunnen constateren (bijvoorbeeld door monitoring).

3.4.3 Notificatie

In Tabel 13 is een overzicht opgenomen van aspecten die ISP's kunnen toepassen ter detectie van botnets.

Tabel 13 Notificatie

Aspect	Naam kenmerk	Omschrijving
N-1	Melding aan geïnfecteerde klanten	Gebruiker informeren over een mogelijke besmetting Dit kan via email, telefoon, in-browser, instantmessaging, SMS of via walled garden bericht.
N-2	Koppeling melding met remediation tools	De melding die de gebruiker in geval van besmetting ontvangt, bevat ook informatie over tools en middelen om het probleem op te lossen.
N-3	Melding aan andere providers	ISP's melden besmettingen aan andere providers.
N-4	Melding ACM	ISP's zijn verplicht om in bepaalde omstandigheden een melding te doen bij de autoriteit ACM.

3.4.4 Verwijdering/bestrijding

In Tabel 14 is een overzicht opgenomen van aspecten die ISP's kunnen toepassen ter verwijdering en bestrijding van botnets.

Tabel 14 Verwijdering/bestrijding

Aspect	Naam kenmerk	Omschrijving
V-1	Isoleren gebruiker	Het plaatsen van geïnfecteerde gebruikers in een zogenaamde 'walled garden'.

V-2	Delen van informatie omtrent het oplossen van een botnetinfectie	ISP's stellen informatie beschikbaar hoe klanten een mogelijke botnetinfectie kunnen oplossen.
V-3	Links naar professionele hulp	De ISP kan klanten informatie geven over waar de klant professionele hulp kan vragen.
V-4	Delen procedure walled garden	De procedure rond het isoleren van besmettingen (walled garden) wordt gedeeld met klanten en andere ISP's zodat voor klanten duidelijk is wanneer zij weer gebruik van hun verbinding kunnen maken.
V-5	Delen best practices verwijdering	ISP's delen informatie met betrekking tot het verwijderen van botnets met andere instanties.

3.4.5 Herstel

In Tabel 15 is een overzicht opgenomen van aspecten die ISP's kunnen toepassen ter herstel van botnets.

Tabel 15 Herstel

Aspect	Naam kenmerk	Omschrijving
H-1	Activeren verbinding klant	De ISP bepaalt op welk moment en hoe een consument weer gebruik kan maken van de internetverbinding nadat de besmetting is verwijderd.
H-2	Ondersteunen van klanten in herstel	ISP's stellen informatie over remediation beschikbaar (dit kan via publicaties of web links) over hoe een klant een botnetinfectie kan oplossen.
H-3	Gevolgen herstel met betrekking tot persoonlijke data en accounts	De ISP informeert de klant welke gevolgen het oplossen van een besmetting heeft met betrekking tot persoonlijke bestanden.
H-4	Informatie herstel	ISP's stellen informatie beschikbaar die klanten kunnen helpen in het herstellen van hun data na het oplossen van een botnetbesmetting.

3.5 Rechten en plichten ISP's

In deze paragraaf wordt geprobeerd om zo helder mogelijk aan te geven wat de rechten en plichten van ISP's zijn in relatie tot botnetbestrijding. Door deze onderbouwing wordt de onderzoeksvraag '***Welke juridische verantwoordelijkheden (rechten en plichten) hebben Internet Service Providers in relatie tot botnetbestrijding?'*** beantwoord.

In de wetenschappelijke literatuur is weinig te vinden over wat ISP's wettelijk verplicht zijn te doen aan botnetbestrijding. Van Eeckhoutte (2010) heeft op 18 februari 2014 een artikel geschreven met de titel "Zorgverplichtingen ISP's tegen internetcriminaliteit". In dit artikel verwijst Van Eeckhoutte naar de Telecommunicatiewet en dan specifiek naar artikel 11.3 van deze wet. In een publicatie van Koops en van der Hof (2002) wordt ook verwezen naar artikel

11.3 van de telecommunicatiewet[2]. Hieronder is artikel 11.3 van de Telecommunicatiewet weergegeven.

Artikel 11.3

1. De in artikel 11.2 bedoelde aanbieders treffen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers passende technische en organisatorische maatregelen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. De maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau dat in verhouding staat tot het desbetreffende risico.

2. De maatregelen als bedoeld in het eerste lid omvatten in elk geval:
   a. waarborgen dat slechts daartoe gemachtigd personeel voor wettelijk toegestane doeleinden toegang heeft tot de persoonsgegevens,
   b. de bescherming van opgeslagen of verzonden persoonsgegevens tegen onbedoelde of niet toegestane opslag, verwerking, toegang, verstrekking, wijziging, verlies, vernietiging, en
   c. de invoering van een veiligheidsbeleid met betrekking tot de verwerking van persoonsgegevens.

3. De in artikel 11.2 bedoelde aanbieders dragen er zorg voor dat de abonnees worden geïnformeerd over:
   a. bijzondere risico's voor de doorbreking van de veiligheid of de beveiliging van het aangeboden netwerk of de aangeboden dienst;
   b. de eventuele middelen waarmee de onder a bedoelde risico's kunnen worden tegengegaan, voor zover het andere maatregelen betreft dan die welke de aanbieder op grond van het eerste lid gehouden is te treffen, alsmede een indicatie van de verwachte kosten.

Volgens Van Eeckhoutte zijn ISP's verplicht om technische en organisatorische maatregelen te treffen ter bescherming tegen onder ander internetcriminaliteit. Concreet betekent dit dat er door de ISP (technische) oplossingen in stelling gebracht moeten worden om een mogelijke inbreuk te voorkomen. Verder geeft van Eeckhoutte ook aan dat de technische vereisten voor bescherming continue strenger dienen te worden omdat de technische kennis en mogelijkheden continue evolueren. Van Eckhoutte zegt hierover: "*Dus, een beveiliging die tien jaar geleden afdoende was volgens de standaarden toentertijd, zal zonder meer nu ondermaats zijn; de veiligheidsnormen liggen tegenwoordig een heel stuk hoger".*

ISP's dienen ervoor te zorgen dat zij hun klanten voldoende informatie vertrekken, zodat die klant zelf een inschatting kan maken welke risico's er kleven aan het gebruik van de internetdiensten van een specifieke ISP. Het gaat dan om risico's zoals spam, virussen en botnets en wat de klant van de ISP hier zelf tegen kan doen om de risico's te verminderen.

[2] Telecommunicatiewet, via http://wetten.overheid.nl/BWBR0009950

Van Eeckhoutte concludeert: "*Op de ISP's rusten dus inspanningsverplichtingen van technische, organisatorische en informatieve aard. Xs4all bijvoorbeeld stelt een checklist ter beschikking waarvan een veiligheidspakket, updates, beveiligingsmodaliteiten en keuze wachtwoord onderdeel van uitmaken. Ook waarschuwt die provider voor nepmails (phishing)".*

Daarnaast is er nog artikel 11.3a van de Telecommunicatiewet. Die is hieronder weergegeven.

Artikel 11.3a

1. De aanbieder van een openbare elektronische communicatiedienst stelt de Autoriteit Consument en Markt onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 11.3, die nadelige gevolgen heeft voor de bescherming van persoonsgegevens die zijn verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Europese Unie.

2. De aanbieder, bedoeld in het eerste lid, stelt degene wiens persoonsgegevens het betreft onverwijld in kennis van een inbreuk in verband met persoonsgegevens indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

3. De kennisgeving aan de Autoriteit Consument en Markt en de persoon wiens persoonsgegevens het betreft, omvat in ieder geval de aard van de inbreuk in verband met persoonsgegevens, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.

   De kennisgeving aan de Autoriteit Consument en Markt omvat tevens de gevolgen van de inbreuk op de persoonsgegevens en de maatregelen die de aanbieder voorstelt of heeft getroffen om de inbreuk aan te pakken.

4. Indien de aanbieder van een openbare elektronische communicatiedienst geen kennisgeving als bedoeld in het tweede lid doet, kan de Autoriteit Consument en Markt, indien het van oordeel is dat de inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de persoon wiens persoonsgegevens het betreft, van de aanbieder verlangen dat hij die persoon alsnog in kennis stelt van de inbreuk.

5. De kennisgeving, bedoeld in het tweede lid, is niet vereist indien de aanbieder naar het oordeel van de Autoriteit Consument en Markt gepaste technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft, versleuteld of anderszins onbegrijpelijk zijn voor een ieder die geen recht heeft op toegang tot die gegevens.

In bovenstaand artikel staat wat ISP's moeten doen als er sprake is van een inbreuk op de beveiliging.

In de expert opinion van Koops (2013) geschreven voor SURFnet staat dat de Telecommunicatiewet niet van toepassing is op SURFnet en dat deze wet alleen geldt voor openbare telecomaanbieders.

Door Houthoff Buruma (2013) wordt ook verwezen naar artikel 11.3a van de Telecommunicatiewet. In dit artikel wordt aangegeven dat de meldplicht sinds 5 juni 2012 van kracht is en geldt voor aanbieders van 'openbare elektronische communicatiediensten'. Door Buruma wordt aangegeven dat ISP's zoals Ziggo, KPN, UPC enz onder deze groep vallen.

In het Cybersecuritybeeld Nederland ((Nationaal Cyber Security Centrum, 2013) staat dat de meldplicht voor datalekken wordt uitgebreid. Er geldt een meldplicht voor verstoringen in de continuïteit van het netwerk van openbare aanbieders voor elektronische communicatienetwerken en –diensten. Met ingang van 5 juni 2012 zijn aanbieders van openbare communicatiediensten ook wettelijk verplicht om beveiligingsincidenten, waarbij de bescherming van persoonsgegevens in het geding is, te melden. Verder staat er in dit Cybersecuritybeeld dat er een nieuw Europees wetvoorstel ligt voor een bredere meldplicht van datalekken waarbij persoonsgegevens zijn betrokken.

Wat ISP's zoals KPN verplicht zijn te doen in geval van een datalek is het doen van een melding aan de Autoriteit Consument en Markt (ACM) en de betrokken klanten informeren als de inbreuk waarschijnlijk nadelige gevolgen zal hebben voor hun privacy (Houthoff Buruma, 2013). In de jaarverslagen van het ACM wordt het aantal meldingen van inbreuk op de beveiliging gemeld. In 2013 waren 211 meldingen en in 2014 is het aantal meldingen gestegen tot 348.

In artikel 11.3 van de Telecommunicatiewet staat niet duidelijk vermeld wat ISP's moeten doen in het geval van ontdekking van een botnet in hun netwerk. Het ontbreekt op dit moment aan een juridisch kader voor ISP's om botnets verplicht aan te pakken. Eigenlijk kan gesteld worden dat de acties die ISP's ondernemen inzake botnetbestrijding op vrijwillige basis zijn.

3.5.1 Hoe ver gaan ISP's in botnetbestrijding?

In 2009 heeft een aantal grote Nederlandse ISP's waaronder KPN, Ziggo, UPC en XS4All een raamwerk/convenant opgesteld met daarin afspraken met betrekking tot botnetbestrijding (ECP, 2009). In deze afspraken is terug te vinden wat ISP's met elkaar hebben afgesproken over botnetbestrijding.

Hieronder de belangrijkste afspraken.

ISP's spreken met elkaar het volgende af:
Informatie vergaring en uitwisseling

I. ISP's houden zich bezig met het vergaren van informatie over botnet-besmettingen in hun netwerk door bijvoorbeeld gebruik te maken van (openbare) externe signaleringssystemen of andere vertrouwde bronnen. Actieve monitoring van het netwerkverkeer van consumenten valt expliciet niet onder deze afspraken.
II. ISP's wisselen op vrijwillige basis onderling informatie uit over het bestaan van, of indicaties over botnetbesmettingen.
III. ISP's wisselen op vrijwillige basis regelmatig expertise en ervaringen uit op het gebied van het abuse-proces en de bestrijding van botnetwerken. ISP's stellen de contactgegevens van hun abuse-afdeling beschikbaar aan de andere mede ondertekenaars.

Aanpak besmetting

IV. Indien een ISP een besmetting constateert, of daarop wordt gewezen door een derde, zal de ISP binnen een redelijke termijn oordelen of hij hiertegen moet optreden. Onder een besmetting wordt verstaan dat een computer, aangesloten op een internetverbinding van één van zijn gebruikers, vermoedelijk onderdeel uitmaakt van een botnetwerk,
V. Indien de ISP een botnet-besmetting binnen zijn eigen netwerk geconstateerd en geverifieerd heeft, zorgt hij er onverwijld voor dat vanaf die internetverbinding een besmette computer niet meer als bot toegang krijgt tot het internet. Op welke wijze dit gebeurt, is aan deze ISP zelf, bijvoorbeeld door de internetverbinding geheel af te sluiten of dit slechts voor een deel te doen ('quarantaine').

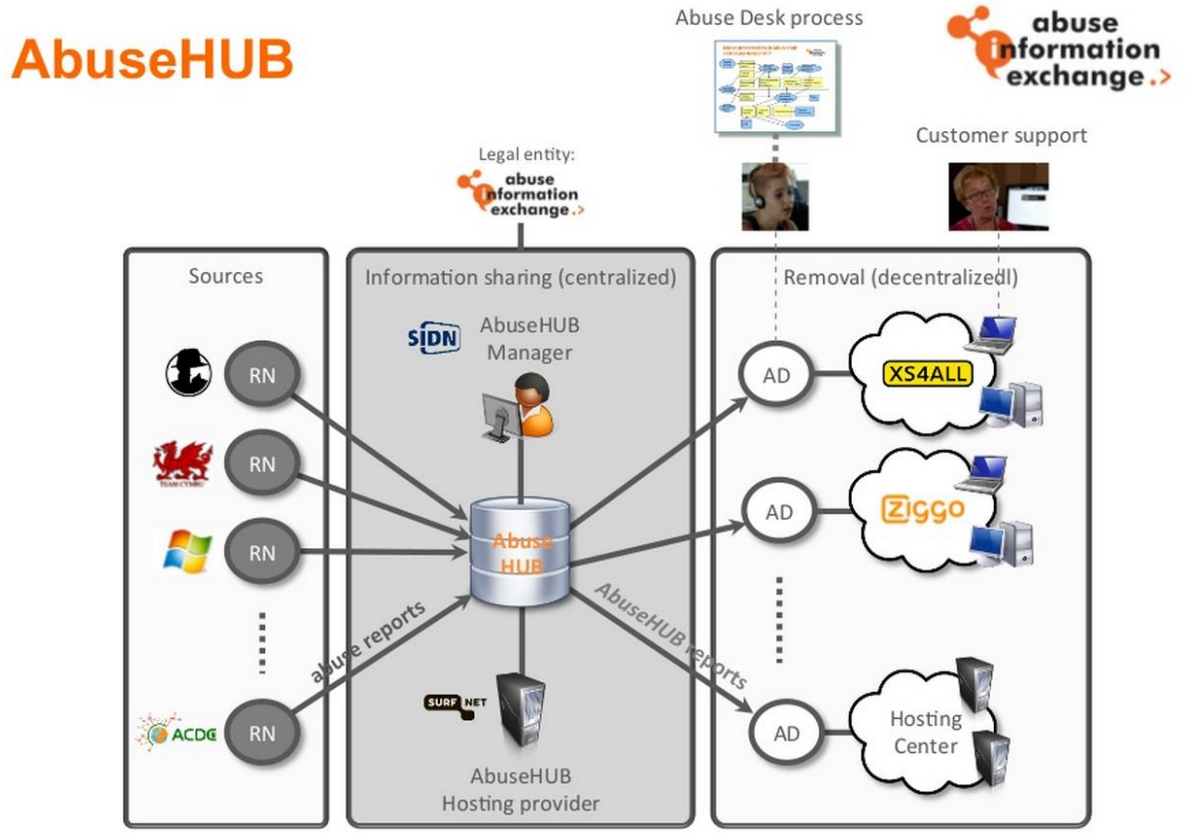
Wat opvalt aan deze afspraken is dat informatie over botnetbesmettingen niet door middel van actieve monitoring tot stand komt. Daarnaast spreken de ISP's af om de internetverbinding van de klant af te sluiten, of dit slechts voor een deel te doen ('quarantaine'), zodat de bot geen toegang meer krijgt tot het internet.

Als er geen gebruik wordt gemaakt van actieve monitoring hoe komen ISP's dan aan informatie over mogelijke besmettingen in hun netwerk? ISP's kunnen informatie van verschillende bronnen zoals de Shadowserver Foundation ontvangen over botnet activiteit in hun netwerk.

Wereldwijd zijn er meerdere instanties/bedrijven die zich bezig houden met de bestrijding en opsporing van botnets. In paragraaf 3.7 worden verschillende samenwerkingsverbanden met betrekking tot botnet bestrijding besproken.

In Nederland is een samenwerking actief genaamd ' Vereniging Abuse Information Exchange'. Deze vereniging heeft een systeem in gebruik genomen genaamd AbuseHUB (Vereniging Abuse Information Exchange 2014). De AbuseHUB verzamelt gegevens van derden over botnetbesmettingen. Deze gegevens worden vervolgens geanalyseerd en verstrekt aan de providers. Vervolgens zijn de providers in staat om hun klanten te informeren over mogelijke besmettingen en de klant in een zogenaamde walled garden omgeving te plaatsen. In Figuur

13 is een schematische weergave opgenomen van de werking van de AbuseHUB (Vereniging Abuse Information Exchange, 2013).



Figuur 13 Schematisch weergaven AbuseHUB

Vanuit de literatuur is het niet duidelijk of ISP's zelf actief botnets opsporen binnen hun eigen netwerk. De meeste ISP's krijgen de informatie over mogelijke besmettingen vanuit externe bronnen.

De vereniging Abuse Information Exchange werkt samen met diverse partijen, die *reliable notifiers* worden genoemd. De databronnen die door de AbuseHUB worden gebruikt kunnen uit binnen- en buitenland komen. In Figuur 13 worden een aantal sources gegeven die door AbuseHUB als input kunnen worden gebruikt. Een voorbeeld van zo een source is bijvoorbeeld Shadowserver. Shadowserver verzamelt onder andere informatie over geïnfecteerde machines binnen een botnet. Deze informatie kan vervolgens door de AbuseHUB worden gedeeld met de ISP waarbinnen zo een geïnfecteerde machine actief is. Vervolgens kan de ISP de benodigde stappen ondernemen.

3.6 Wat doen ISP's afzonderlijk

In deze paragraaf wordt een beeld geschetst van wat de ISP's afzonderlijk van elkaar doen aan botnetbestrijding. Hiermee wordt onderzoeksvraag ***'Wat doen Internet Service Providers afzonderlijk van elkaar aan botnetbestrijding?'*** beantwoord.

In de literatuur is er gezocht naar wat individuele providers afzonderlijk van elkaar doen aan botnetbestrijding. Wat opvalt in de literatuur is dat er veel geschreven is over wat ISP's kunnen bijdragen aan botnetbestrijding, maar niet wat de ISP's afzonderlijk van elkaar doen aan botnetbestrijding.

Volgens het artikel Toward Incentivinzing ISP's To Mitigate Botnets (van Eeten et al., 2014) vormen ISP's een centraal punt om botnetinfecties te reguleren. ISP's worden niet gestimuleerd om te investeren in botnetbestrijding. Wat het effect van botnetbestrijding is, kan niet worden vastgesteld zonder nauwkeurige en betrouwbare metingen.

Uit onderzoek door van Eeten en Bauer (2008) kwam naar voren dat bij een grote Europese ISP, die vier miljoen klanten bedient, de ISP per maand met 1000 klanten contact opneemt, omdat ze slachtoffer zijn geworden van botnet/malware. Onderzoekers schatten het totaal aan geïnfecteerde machines op vijf procent. Dit zou beteken dat er tussen de 40.000 en 200.000 geïnfecteerde machines op het netwerk van deze ISP zijn aangesloten.

Over de aanpak van SURFnet inzake botnetbestrijding is het meeste gepubliceerd (binnen Nederland). SURFnet heeft ervoor gekozen om in 2013 gedragscodes te ontwikkelen rondom anti-botnetacties (SURFnet, 2013). Om tot goed onderbouwde gedragscodes te komen heeft SURFnet twee Hoogleraren van Tilburg Institue of Law (TILT) gevraagd een expert opinion te schrijven.
Prof. Dr. Bert-Jaap Koops heeft zijn mening opgeschreven ten aanzien van strafrechtelijke aspecten van anti-botnetacties door SURFnet en bij SURFnet aangesloten instellingen (Koops, 2013). Daarnaast heeft prof. Dr. Ronald Leenes een expert opinion geschreven ten aanzien van mogelijke privacy inbreuken die anti-botnetacties en het daarbij beschikbaar komen van "gestolen" data met zich meebrengen (Leenes, 2013). Deze gedragscodes zijn gepresenteerd tijdens de TERENA Networking Conference (TNC).

Binnen SURF is SURFcert actief. SURFcert is het Computer Security Incident Team (CSIRT) van SURFnet. SURFcert biedt 24 uur per dag en 7 dagen per week ondersteuning bij beveiligingsincidenten aan instellingen die zijn aangesloten op het SURFnet. SURFcert onderzoekt en coördineert bij beveiligingsinbreuken. Daarnaast helpt SURFcert ook bij het opzetten van lokale CERT-teams bij SURFnet aangesloten instellingen.

De meeste providers binnen Nederland hebben een abuse afdeling waar klanten met problemen terecht kunnen. De meeste providers kunnen bij misbruik van de verbinding van de klant deze ook isoleren in een zogenaamde walled garden.

Volgens een artikel van Jacobs (Jacobs, 2013) doen alle grote providers aan 'egress' filtering.

In de literatuur is niet terug te vinden wat de individuele providers afzonderlijk van elkaar doen aan botnetbestrijding. Daarnaast zijn er nagenoeg ook geen cijfers bekend van het aantal klanten dat per jaar bij een bepaalde provider in een zogenaamde walled garden wordt geplaatst. Daarnaast is het natuurlijk interessant om te weten of providers klanten actief in een walled garden plaatsen. Op het moment dat een provider er voor kiest om een klant, die is besmet met malware, in een walled garden te plaatsen, neemt deze klant waarschijnlijk

contact op met de helpdesk van de provider. Het actief plaatsen van klanten in een walled garden brengt op deze manier kosten met zich mee.

In recente literatuur is niet te vinden hoe ver ISP's gaan in botnetbestrijding. Wel zijn er verschillende samenwerkingsinitiatieven en afspraken, die ISP's onderling hebben gemaakt, terug te vinden. Het blijft onduidelijk of ISP's actief op zoek gaan naar botnetbesmettingen in hun netwerk.

3.7 Samenwerkingsinitiatieven op het gebied van botnetbestrijding

In deze paragraaf wordt een beeld geschetst van bestaande samenwerkingsinitiatieven met betrekking tot botnetbestrijding. Hiermee wordt de onderzoeksvraag '***Welke samenwerkingsinitiatieven zijn er te vinden over hoe Internet Service Providers samenwerken met andere partijen met betrekking tot botnetbestrijding?'*** beantwoord.

Op het gebied van botnetbestrijding zijn meerdere samenwerkingsverbanden en initiatieven te vinden (Oecd, 2012; Plohmann et al., 2011; Tiirmaa-Klaar et al., 2013). In Tabel 16 is een overzicht opgenomen van initiatieven met betrekking tot botnetbestrijding, zoals bekend in de literatuur.

Door Tiirmaa-Klaar et al. (2013) wordt als globaal initiatief het 'Botnet Mitigation and Remediation Special Interest Group' genoemd. Deze groep is gestart als onderdeel van 'Forum of Incident Response and Security Teams (FIRST)'. Het doel van deze groep is het bestuderen van verschillende initiatieven wereldwijd met betrekking tot het bestrijden van botnets en malware.

Tabel 16 Initiatieven botnetbestrijding

Naam initiatief	Land	Link
iCode	Australie	http://www.commsalliance.com.au/Activities/ispi
Anti-Botnet Beratungszentrum	Duitsland	https://www.botfrei.de/
Irish Anti-Botnet Initiative	Ierland	https://www.botfrei.de/ie/
Cyber Clean Center (CCC)	Japan	https://www.telecom-isac.jp/ccc/en_index.html
Cyber Curing System / e-Call Center 118	Korea	http://eng.krcert.or.kr/service/cyber.jsp
Autoreporter	Finland	https://www.viestintavirasto.fi
Swiss Internet Security Alliance	Zwitersland	https://www.swiss-isa.ch
Anti-Botnet Working Group	Nederland	https://ecp.nl/werkgroep-botnets
Abuse Information Exchange	Nederland	https://www.abuseinformationexchange.nl/
ACDC – Advanced Cyber Defence Center	Europa	http://www.acdc-project.eu/ http://botfree.eu/
Online Trust Alliance ABC's for ISP's	Wereldwijd	https://otalliance.org/resources/botnets

3.7.1 Australië

Door van van Eeten et al. (2010) wordt er verwezen naar een initiatief van de Australische regering waarin de Australian Communications and Media Authority (ACMA) een clearinghouse heeft opgezet die meerdere data feeds samenvoegt en omzet naar wekelijkse rapporten voor Australische ISP's. Door ACMA is de Australian Internet Security Initiative (AISI) opgezet. De AISI is begonnen met zes Australische providers. Op dit moment heeft AISI 139 leden (waaronder 18 universiteiten). Met dit aantal leden bestrijkt de AISI 98 procent van de Australische IP range.

Op de website van ACMA wordt aangegeven wat AISI doet. AISI verzamelt gegevens van verschillende bronnen over computers die zich gedragen als 'bot' op het Australische internet. Deze data worden door ACMA gebruikt om op een dagelijkse basis rapporten te verzenden naar de leden. Vervolgens kunnen ISP's hun klanten informeren dat hun machine waarschijnlijk is overgenomen en hoe ze dit kunnen oplossen.

Tot 27 mei 2014 zijn er in totaal 8.52 miljoen infecties gerapporteerd aan de deelnemers van de AISI. Gemiddeld werden er in het jaar 2013 – 2014 per dag 25.839 infecties gerapporteerd. In het voorgaande jaar (2012 – 2013) waren dat er 16.034.

Op 28 november 2014 is er op de website security.nl een artikel geplaatst over de aanpak van malware bestrijding in Australië en dat er door ACMA een nieuw online portal is geopend (Security.NL, 2014). De informatie die security.nl gebruikt voor het artikel is overgenomen van een item op de website van de ACMA (Australian Communications and Media Authority, 2014).

Wat opvalt in het samenwerkingsinitiatief in Australië is dat het een samenwerking is tussen publieke en private partijen. De ISP's in Australië hebben een code geaccepteerd die is voorgesteld door Internet Industry Association (IIA). Deze code heeft tot doel (Communications Alliance, 2014):

- Zorgen dat cyber-security onder de aandacht is van de Australische ISP's en haar klanten
- Zorgen voor uniforme berichtgeving in normale bewoording naar haar klanten
- Klanten assisteren waarvan apparaten zijn geïnfecteerd en daarnaast een strategie ontwikkelen waardoor andere gebruikers van het netwerk van de ISP hier geen hinder van ondervinden
- ISP's aan te moedigen om geïnfecteerde machines te identificeren in hun netwerk
- ISP's aan te moedigen om met elkaar in gesprek te gaan en incidenten te melden die invloed hebben op de kritische infrastructuur van Australië of invloed hebben op een nationaal security niveau
- Bovenstaande punten zo te implementeren dat de privacy van de klanten gewaarborgd blijft.

Wat verder opvalt in de Australische aanpak is dat er aandacht wordt besteed aan preventie. Dit komt tot uiting in initiatieven zoals "cyber (smart:)", waarin de Australische overheid betrokken is en de ACMA.

3.7.2 Initiatieven binnen Nederland

In de media is de afgelopen jaren meerdere malen melding gemaakt van initiatieven van samenwerkingen tussen partijen uit de private sector en de publieke sector. In Tabel 17 is een overzicht van een aantal van deze samenwerkingen opgenomen.

Tabel 17 Initiatieven botnetbestrijding Nederland

Naam initiatief	Jaar gestart
Werkgroep Botnets binnen het platform Internetveiligheid (ECP)	2009
Abuse Information Exchange	2012

In 2009 heeft een aantal Nederlands ISP's een anti-botnet convenant met elkaar afgesloten.

Wat opvalt, is het feit dat er in de media meerdere meldingen worden gedaan van initiatieven van oprichting van bijvoorbeeld werkgroepen die aan de slag gaan met botnetbestrijding. Er worden echter in de media nauwelijks tot geen resultaten door deze groepen gedeeld.

In Nederland is een neutraal platform genaamd ECP actief waarin bedrijfsleven, overheid en maatschappelijke organisaties tot doel hebben het gebruik van ICT in de Nederlandse samenleving te versterken. Sinds 2009 is binnen het ECP het Platform Internetveiligheid actief. Dit platform heeft als doel een structurele bijdrage te leveren aan het verbeteren van de internetveiligheid voor de consument/internetgebruiker. Het richt zich op strategische onderwerpen in relatie tot internetveiligheid en streeft naar een agenderende en voorbeeldfunctie door maatschappelijke trends te signaleren en te vertalen naar concrete initiatieven. Binnen het Platform Internetveiligheid zijn enkele werkgroepen actief. Eén daarvan is de werkgroep Botnetproject.

De werkgroep Botnets binnen het Platform Internetveiligheid heeft een doel geformuleerd en een aantal activiteiten benoemd. Het doel van de werkgroep is om binnen en vanuit Nederland een structurele bijdrage te leveren aan de bestrijding van botnets en het tegengaan van de negatieve gevolgen ervan. Onder andere door eigen acties van deelnemers, maar ook door overzicht te houden op en waar mogelijk coördineren van andere activiteiten.

In het jaarverslag 2014 – 2015 van het ECP wordt er gesproken over een revolutionaire samenwerking op het gebied van veilig internet (ECP, 2015). De ECP verwijst hiermee naar het feit dat de marktpartijen de handen ineen hebben geslagen in vereniging Abuse Information Exchange om besmettingen vanuit verschillende bronnen op een centraal punt te verzamelen en te valideren. Daardoor kunnen botnetbesmettingen sneller en beter bestreden worden, waarmee de veiligheid en stabiliteit van het internet volgens het ECP wordt verbeterd. Het ECP meldt verder nog dat er binnen de vereniging Abuse Information Exchange samengewerkt wordt met het NCSC en dat het in gesprek is met verschillende ministeries over hoe de bestrijding van botnets in de gehele keten het beste kan worden aangepakt.

In Cybersecuritybeeld Nederland CSBN-2 staat dat een aantal Nederlandse ISP's en andere marktpartijen zich hebben verenigd in de Werkgroep Botnets (Nationaal Cyber Security

Centrum, 2012). De deelnemers hebben de afspraken vastgelegd in een convenant. Voor de aanpak van infecties bij klanten heeft het kabinet vorig jaar in deze werkgroep voorgesteld om een ‘clearing house’ op te zetten. Hiermee kunnen ISP’s klanten informeren die besmet zijn en hen helpen om hun computers te ontsmetten en schoon te houden. Het ‘clearing house’ is daarmee een belangrijke schakel in de opsporing en ontsmetting van botnets.

In het Cybersecuritybeeld Nederland CSBN-3 wordt aandacht besteed aan de samenwerking abusemeldingen in telecom. In oktober 2012 werd de Abuse Information Exchange opgericht door internetproviders KPN, SOLCON, Tele2, UPC, XS4ALL, Zeelandnet en Ziggo, SIDN, de .nl-registry en ECP, Platform voor de Informatiesamenleving.
In november 2013 is officieel de AbuseHUB in gebruik genomen door de vereniging Abuse Information Exchange. De AbuseHUB is een systeem dat centraal informatie verwerkt over botnetbesmettingen in Nederland, met als doel besmette computers sneller te detecteren en internetgebruikers beter en sneller te helpen.

Interessant is wat de AbuseHUB tot nu toe heeft opgeleverd. Tijdens het ISD congres in september 2014 is er een presentatie geweest over de AbuseHUB en de werking hiervan. In de presentatie is een sheet opgenomen over de toegevoegde waarde van de AbuseHUB. Op dit moment zijn er nog geen werkelijke cijfers en feiten bekend van de opbrengst van de AbuseHUB. Door het samenwerkingsverband is er wel een impact evaluatie aangekondigd, die zal worden uitgevoerd door Delft University of Technology.

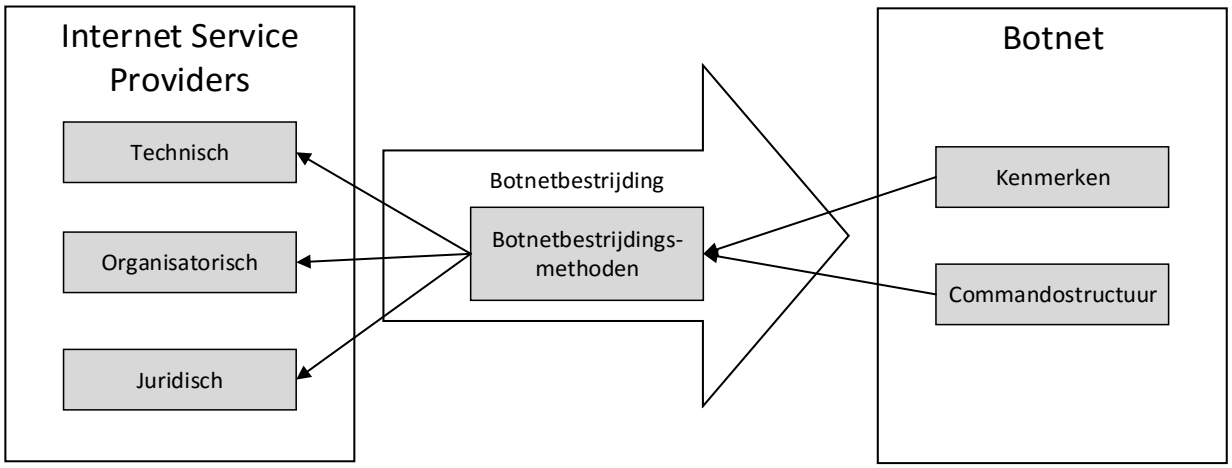
4 Conceptueel model en referentiemodel voor botnetbestrijding door ISP's

De uitkomsten van het literatuuronderzoek zijn te vatten in een conceptueel model en in een referentiemodel. In dit hoofdstuk wordt eerst het conceptueel model beschreven om vervolgens dit model te concretiseren naar een referentiemodel.

4.1 Conceptueel model

In

Figuur 14 is het conceptueel model opgenomen. In dit conceptueel model worden de kernbegrippen van het onderzoek weergegeven en tevens laat het model zien hoe de relevante aspecten van het onderzoek samenhangen. De samenhang kan als volgt worden beschreven: de kenmerken van een botnet en van de commandostructuur zijn de twee eigenschappen die bepalend zijn voor de bestrijdingsmethoden van een botnet, die vervolgens bepaalde technische, organisatorische en/of juridische maatregelen vereisen van de betrokken ISP's.



Figuur 14 Conceptueel model

4.2 Theoretische referentiemodel

Het referentiemodel kan worden gezien als een concretisering van het conceptueel model. Het referentiemodel is opgedeeld in vijf verschillende hoofdgebieden. Deze hoofdgebieden vormen samen de anti-botnet life cycle. De stappen die een ISP kan uitvoeren volgens de anti-botnet life cycle zijn:

- Preventie maatregelen
- Detectie
- Informeren
- Oplossen
- Herstel

Vervolgens is er per stap een aantal aspecten benoemd die een ISP kan ondernemen in de strijd tegen botnets. Een aspect kan technisch, organisatorisch of juridisch van aard zijn. Daarnaast heeft een bepaald aspect één of meerdere doelgroepen. In Tabel 18is het opgestelde theoretisch referentiemodel opgenomen.

Tabel 18 Theoretisch referentiemodel

Doelgroep	Aspect	Naam kenmerk	Omschrijving	Technisch	Organisatorisch	Juridisch
Preventie						
Klant	P-1	Beschikbaar stellen end-point security	ISP's stellen end-point security oplossingen beschikbaar voor hun klanten. Dit kan bijvoorbeeld door klanten een antivirussoftware aan te bieden of een router met beveiliging.	x	x	
	P-2	Educatie van klanten	Door ISP's wordt er actief uitleg gegeven over het gevaar van botnets en de acties die klanten kunnen ondernemen om dit te voorkomen. Hierbij valt te denken aan: waarom klanten hun software up-to-date moeten houden, bewustwording campagnes, aanmoedigen van klanten om een end-point security oplossing te gebruiken, belang van backups en acties die klanten kunnen ondernemen om niet onderdeel te worden van een botnet. Eén van de doelen van educatie van klanten is de volgende: dat er bij de klant bewustwording ontstaat dat hij mede verantwoordelijk is in het voorkomen van een botnetbesmetting (gedeelde verantwoordelijkheid).	x	x	x
Andere partijen	P-3	Delen/communiceren van informatie/procedures omtrent botnetbestrijding	Door ISP's wordt er actief gecommuniceerd met andere stakeholders. Door ISP's wordt bijvoorbeeld informatie gedeeld met andere stakeholders over lessons-learned en procedures inzake botnetbestrijding.		x	
	P-4	Deelnemen in een samenwerkingsverband inzake botnetbestrijding	Door ISP's wordt actief deelgenomen in samenwerkingsverbanden met betrekking tot botnetbestrijding.		x	
ISP intern	P-5	Intrusion Prevention Systems (IPS)	ISP's maken gebruik van Intrusion Prevention Systems (IPS) om botnetbesmettingen te kunnen voorkomen.	x		
	P-6	Nemen van technische maatregelen inzake botnets	ISP's kunnen een aantal technische maatregelen nemen zodat het moeilijker wordt voor een botnet om machines te infecteren. Bijvoorbeeld het beveiligen van DNS servers.	x		
	P-7	Bijhouden stand van zaken met betrekking tot botnet/malware technieken.	ISP's blijven op de hoogte van de laatste ontwikkelingen met betrekking tot botnets en malware. Bijvoorbeeld door het trainen van personeel met betrekking tot bestrijding en detectie van botnets.	x	x	
	P-8	Klant support processen	Door de ISP's zijn er processen ingericht omtrent klantondersteuning inzake botnetbesmettingen.		x	
	P-9	Abuse team	ISP's hebben een abuse team actief.		x	
	P-10	Service Level Agreements	ISP's richten Service Level Agreements in met betrekking tot botnetbestrijding.		x	

	P-11	Standaardisering	Voldoen aan internationale standaarden inzake beveiliging (ISO 27002:2005, ISO 27006:2007)		x	
Detectie						
Klant	D-1	Aanbieden self-identify portal	Gebruikers zelf via tools, web portal of andere resource een mogelijke infectie laten vaststellen		x	
	D-2	Ontvangen informatie over mogelijke besmettingen via klanten	ISP's kunnen van klanten informatie krijgen over besmettingen binnen hun netwerk.		x	
Andere partijen	D-3	Communiceren gedetecteerde besmettingen	ISP's delen informatie over gedetecteerde besmettingen met andere ISP's.		x	
	D-4	Ontvangen informatie over mogelijke besmettingen via externe partijen	ISP's kunnen informatie over kwaadaardige activiteiten en bot geïnfecteerde klanten krijgen van externe partijen.		x	
	D-5	Ontvangen informatie over mogelijke besmettingen via AbuseHUB	ISP's ontvangen informatie over mogelijke besmettingen vanuit het AbuseHUB systeem.		x	
ISP intern	D-6	Honeynet	ISP's maken gebruik van honeypots om besmettingen in het netwerk te kunnen constateren.	x		
	D-7	Detectie besmetting	Als een besmetting wordt geconstateerd, of daarop wordt gewezen door een derde, zal de ISP binnen een redelijke termijn beoordelen of hij hier tegen moet optreden.	x		
	D-8	Intrusion Detection Systems (IDS)	ISP's maken gebruik van Intrusion Detection Systems (IDS) om botnetbesmettingen te kunnen constateren (bijvoorbeeld door monitoring).	x		
Notificatie						
Klant	N-1	Melding aan geïnfecteerde klanten	Gebruiker informeren over een mogelijke besmetting Dit kan via email, telefoon, in-browser, instantmessaging, SMS of via walled garden bericht.		x	
	N-2	Koppeling melding met remediation tools	De melding die de gebruiker in geval van besmetting ontvangt, bevat ook informatie over tools en middelen om het probleem op te lossen.	x	x	
Andere partijen	N-3	Melding aan andere providers	ISP's melden besmettingen aan andere providers.		x	
	N-4	Melding ACM	ISP's zijn verplicht om in bepaalde omstandigheden een melding te doen bij de autoriteit ACM.		x	x
Verwijdering/bestrijding						
Klant	V-1	Isoleren gebruiker	Het plaatsen van geïnfecteerde gebruikers in een zogenaamde 'walled garden'.	x	x	
	V-2	Delen van informatie omtrent het oplossen van een botnetinfectie	ISP's stellen informatie beschikbaar hoe klanten een mogelijke botnetinfectie kunnen oplossen.	x	x	
	V-3	Links naar professionele hulp	De ISP kan klanten informatie geven over waar de klant professionele hulp kan vragen.		x	
Klant / Andere partijen	V-4	Delen procedure walled garden	De procedure rond het isoleren van besmettingen (walled garden) wordt gedeeld met klanten en andere ISP's zodat voor klanten duidelijk is wanneer zij weer gebruik van hun verbinding kunnen maken.		x	
Andere partijen	V-5	Delen best practices verwijdering	ISP's delen informatie met betrekking tot het verwijderen van botnets met andere instanties.		x	
Herstel						

Klant	H-1	Activeren verbinding klant	De ISP bepaalt op welk moment en hoe een consument weer gebruik kan maken van de internetverbinding nadat de besmetting is verwijderd.	x	x	
	H-2	Ondersteunen van klanten in herstel	ISP's stellen informatie over remediation beschikbaar (dit kan via publicaties of web links) over hoe een klant een botnetinfectie kan oplossen.		x	
	H-3	Gevolgen herstel met betrekking tot persoonlijke data en accounts	De ISP informeert de klant welke gevolgen het oplossen van een besmetting heeft met betrekking tot persoonlijke bestanden.		x	
	H-4	Informatie herstel	ISP's stellen informatie beschikbaar die klanten kunnen helpen in het herstellen van hun data na het oplossen van een botnetbesmetting.		x	

5 Empirische Onderzoeksresultaten

Op basis van de literatuur is er een theoretisch referentiemodel samengesteld dat tijdens de empirische fase is getoetst. In dit hoofdstuk zullen de empirische onderzoeksvragen worden beantwoord op basis van de resultaten van de semigestructureerde interviews. De goedgekeurde geanonimiseerde interviews met de verschillende ISP's zijn terug te vinden in bijlage 5. In bijlage 5 is tevens het interview opgenomen dat is afgenomen bij een adviseur van het NCSC. Met het NCSC is het opgestelde referentiemodel doorgenomen. Echter, was het voor het NCSC niet mogelijk om aan te geven wat ISP's specifiek doen aan botnetbestrijding omdat zij zichzelf enkel zien in een adviserende rol. Het NCSC wil geen oordeel geven over hoe ISP's botnetbestrijding aanpakken. Het NCSC heeft wel aangegeven wat zij belangrijk acht in de strijd tegen botnets. Daarom zijn de aspecten van het referentiemodel beoordeeld op prioriteit.

5.1 Semigestructureerde interviews

In totaal zijn er zes interviews uitgevoerd. Vijf interviews bij ISP's die binnen Nederland actief zijn. Het zesde interview is ter verificatie uitgevoerd bij het NCSC.

5.2 Beantwoording empirische onderzoeksvragen

In de volgende paragrafen worden de empirische onderzoeksvragen beantwoord.

5.2.1 Wat wordt door ISP's verstaan onder botnets?

In Tabel 19 zijn de antwoorden van de verschillende ISP's opgenomen over de definitie van botnets die wordt gehanteerd door de ISP's.

Tabel 19 Definities botnets ISP's

ISP	Definitie botnet
ISP1	Een netwerk van computers/apparaten die van afstand bestuurd worden vanaf een centraal punt (Centraal punt is tegenwoordig ook P2P) en die kunnen worden ingezet voor cybercriminaliteit.
ISP2	Een botnet is een netwerk van systemen die ongewenst op afstand beheerd/bestuurd worden.
ISP3	Door de ISP wordt er geen definitie gehanteerd. Er wordt gekeken of iets mogelijk besmet is en hier wordt melding van gemaakt.
ISP4	Botnets zijn computers die centraal worden aangestuurd en die samenwerken. Het doel hiervan is dat de besmette machines misbruikt worden voor bijvoorbeeld een DDoS aanval.
ISP5	Botnet is een netwerk van samenwerkende apparaten die zijn geïnfecteerd (onvrijwillig) met (dezelfde) malware en onder controle staan van een persoon of organisatie en die gecoördineerd cyberaanvallen kunnen uitvoeren.

Uit Tabel 19 blijkt dat geen enkele ISP's dezelfde definitie hanteert voor botnets. Echter, de definities komen allemaal op het zelfde neer.

5.2.2 Hoe worden botnets geclassificeerd door ISP's?

Nadat een botnet is gedetecteerd, is het mogelijk om een botnet te classificeren. Een mogelijke classificatie voor botnets is de classificatie op basis van de commandostructuur zoals veelvuldig in de literatuur wordt toegepast. In de interviews wordt door alle ISP's aangegeven, dat waar een classificatie wordt toegepast, dit in de meeste gevallen een eigen classificatie is. Hierdoor is de wijze van classificatie van botnets heel divers. In Tabel 20 is een overzicht opgenomen met daarin de wijze waarop ISP's botnets classificeren.

Tabel 20 Classificatie botnets

ISP	Classificatie botnets
ISP1	Door de ISP worden botnets geclassificeerd. De classificatie richt zich vooral op wie er gevaar loopt, bijvoorbeeld de klant, de ISP en het netwerk.
ISP2	Door de ISP worden botnets niet geclassificeerd. Als de ISP een botnet bestrijdt, is dit altijd in samenwerking met NCSC. NCSC heeft dan de botnet geclassificeerd. De ISP classificeert wel abuse, maar geen botnets.
ISP3	Door de ISP wordt er geclassificeerd op de volgende wijze: geïnfecteerd of niet geïnfecteerd.
ISP4	De ISP geeft aan dat botnets zelf niet specifiek worden geclassificeerd, maar besmettingen in het algemeen wel. De volgende kwalificaties worden gebruikt: - De klant is een gevaar voor anderen. - De klant heeft alleen zelf een probleem. - De klant is kwetsbaar en kan mogelijk geïnfecteerd raken waarna hij een gevaar voor anderen kan worden.
ISP5	Door de ISP wordt aangegeven dat een klant geïnfecteerd kan zijn of niet geïnfecteerd kan zijn. Er wordt niet specifiek een classificatie toegepast voor botnets.

5.2.3 Aan welke samenwerkingsverbanden worden door ISP's deelgenomen?

Door het merendeel van de ISP's wordt deelgenomen aan een samenwerkingsverbanden. Vier van de vijf ISP's zijn onderdeel van de Vereniging Abuse Information Exchange. Door ISP5 wordt aangegeven dat zij hier binnenkort ook onderdeel van willen zijn. Tijdens de literatuurstudie is een diversiteit aan samenwerkingsverbanden gevonden waar ISP's aan deelnemen. In Tabel 21 is een overzicht opgenomen met daarin het antwoord van de verschillende ISP's op de vraag aan welke samenwerkingsverbanden wordt deelgenomen.

Door ISP3 wordt aangegeven dat ze onderdeel uitmaken van het operationeel Incident Response Team overleg (o-IRT-o). Dit samenwerkingsverband wordt in de literatuur nagenoeg niet genoemd in relatie tot botnetbestrijding.

Tabel 21 Deelname samenwerkingsverbanden

ISP	Deelname samenwerkingsverbanden
ISP1	Forum for Incident Response and Security Teams (First) - Internationaal The IT Association for Telecommunications (ETIS) Binnen Nederland actief in verschillende overlegorganen mede opgezet door de overheid (Nationaal Cyber Security Centrum) Vereniging Abuse Information Exchange
ISP2	Vereniging Abuse Information Exchange
ISP3	The honeynet project / honeyned chapter Nederland o-IRT-o Vereniging Abuse information Exchange First Squid
ISP4	Vereniging Abuse Information Exchange
ISP5	Geen

5.2.4 Is het opgestelde theoretische referentiemodel compleet?

Door de verschillende ISP's wordt aangegeven dat het referentiemodel compleet is. Echter, is er een aantal zaken die niet worden toegepast. Een voorbeeld hiervan is aspect P-5 Intrusion Prevention System (IPS). Door alle ISP's werd aangegeven dat er geen IPS actief is in hun netwerk voor klantverkeer. Hetzelfde geldt voor aspect D-8 Intrusion Detection System. Door alle ISP's werd er met klem aangegeven dat ze niet in het verkeer van klant meekijken.

Door de ISP's wordt aangegeven dat het referentiemodel compleet is. Er is echter in het referentiemodel een aantal aspecten opgenomen die door de ISP's niet worden uitgevoerd of welke nog een wens voor de toekomst zijn.

5.2.5 Is het opgestelde theoretische referentiemodel correct?

Door de ISP's en NCSC wordt aangegeven dat het referentiemodel in hoofdlijnen correct is.

Met de verschillende partijen is het referentiemodel doorlopen en zijn de opmerkingen verwerkt in de vraagverwerkingslijst. In Tabel 22 is de vergelijkingstabel opgenomen. In de laatste kolom is de input van het NCSC verwerkt. Door het NCSC is per aspect middels een vijfpuntschaal een score gegeven. In deze schaal is één het laagste en vijf het hoogste. Wat hierin opvalt, is de score die wordt gegeven aan P1 en P2. Door het NCSC wordt aangegeven dat het bestrijden van het botnetprobleem begint bij de klant.

Tabel 22 Vergelijkingstabel referentiemodel

Doelgroep	Aspect	Naam kenmerk	Technisch	Organisatorisch	Juridisch	ISP1	ISP2	ISP3	ISP4	ISP5	NCSC
Preventie											
Klant	P-1	Beschikbaar stellen end-point security	x	x		Ja	Ja	Beperkt	Ja	Ja	5
	P-2	Educatie van klanten	x	x	x	Ja	Ja	Ja	Ja	Ja	5
Andere partijen	P-3	Delen/communiceren van informatie/procedures omtrent botnetbestrijding		x		Ja	Ja	Ja	Ja	Nee	4
	P-4	Deelnemen in een samenwerkingsverband inzake botnetbestrijding		x		Ja	Ja	Ja	Ja	Nee	5
ISP intern	P-5	Intrusion Prevention Systems (IPS)	x			Nee	Nee	Nee	Nee	Wens	
	P-6	Nemen van technische maatregelen inzake botnets	x			Nee	Beperkt	Nee	Ja	Ja	5
	P-7	Bijhouden stand van zaken met betrekking tot botnet/malware technieken.	x	x		Beperkt	Ja	Ja	Beperkt	Ja	3
	P-8	Klant support processen		x		Ja	Ja	Ja	Ja	Ja	3
	P-9	Abuse team		x		Ja	Ja	Ja	Ja	Ja	3
	P-10	Service Level Agreements		x		Ja	Nee	Ja	Nee	Nee	
	P-11	Standaardisering		x		Ja	Wens	Beperkt	Ja	Nee	1
Detectie											
Klant	D-1	Aanbieden self-identify portal		x		Beperkt	Beperkt	Nee	Nee	Nee	5
	D-2	Ontvangen informatie over mogelijke besmettingen via klanten		x		Ja	Nee	Beperkt	Nee	Nee	2
Andere partijen	D-3	Communiceren gedetecteerde besmettingen		x		Nee	Ja	Ja	Beperkt	Nee	4
	D-4	Ontvangen informatie over mogelijke besmettingen via externe partijen		x		Ja	Ja	Ja	Ja	Ja	4
	D-5	Ontvangen informatie over mogelijke besmettingen via AbuseHUB		x		Ja	Ja	Ja	Ja	Nee	5
ISP intern	D-6	Honeynet	x			Nee	Ja	Nee	Beperkt	Nee	4
	D-7	Detectie besmetting	x			Ja	Ja	Ja	Ja	Nee	3
	D-8	Intrusion Detection Systems (IDS)	x			Nee	Nee	Beperkt		Wens	
Notificatie											

Klant	N-1	Melding aan geïnfecteerde klanten		x		Ja	Ja	Ja	Ja	Ja	5
	N-2	Koppeling melding met remediation tools	x	x		Ja	Ja	Beperkt	Ja	Ja	5
Andere partijen	N-3	Melding aan andere providers		x		Nee	Ja	Ja	Beperkt	Nee	4
	N-4	Melding ACM		x	x	Nee	Nee	Nee	Ja	Nee	
Verwijdering/bestrijding											
Klant	V-1	Isoleren gebruiker	x	x		Ja	Ja	Nee	Ja	Nee	5
	V-2	Delen van informatie omtrent het oplossen van een botnetinfectie	x	x		Ja	Ja	Ja	Ja	Ja	5
	V-3	Links naar professionele hulp		x		Ja	Beperkt	Nee	Nee	Ja	4
Klant / Andere partijen	V-4	Delen procedure walled garden		x		Ja	Ja	Nee	Ja	Nee	3
Andere partijen	V-5	Delen best practices verwijdering		x		Ja	Nee	Ja	Beperkt	Nee	3
Herstel											
Klant	H-1	Activeren verbinding klant	x	x		Ja	Ja	Nee	Ja	Ja	4
	H-2	Ondersteunen van klanten in herstel		x		Nee	Ja	Nee	Beperkt	Ja	4
	H-3	Gevolgen herstel met betrekking tot persoonlijke data en accounts		x		Ja	Ja	Nee	Beperkt	Ja	3
	H-4	Informatie herstel		x		Nee	Beperkt	Nee	Beperkt	Nee	3

5.2.5.1 Extra

Tijdens het interview met de verschillende partijen is er een aantal zaken extra meegenomen. Zo is er aan de hand van de in Tabel 23 opgenomen lijst getoetst of ISP's bepaalde zaken niet toepassen in de strijd tegen botnets. Daarnaast is er gekeken welke zaken op dit moment effectief zijn tegen botnets en welke zaken in de toekomst effectief kunnen zijn. Tot slot is er nog gevraagd op welk onderdeel van een botnet ISP's zich richten in de strijd tegen botnets.

In Tabel 23 is de lijst opgenomen met niet ISP gerelateerde botnetbestrijdingsmethoden. Door de verschillende ISP's wordt aangegeven dat dit niet door hen wordt toegepast in de strijd tegen botnets. Bovenstaand wordt bevestigd door het NCSC.

Tabel 23 Niet ISP gerelateerde botnetbestrijdingsmethoden

Techniek	Omschrijving
Takedown	Het achterhalen en neerhalen van botnets.
Hack-back	Het overnemen van command and control servers om zo een botnet van binnenuit te bestrijden.
Infiltreren/manipuleren botnet	Het infiltreren in een botnet om de botnet zo van binnenuit te manipuleren.

Desinfecteren klant machine	Het op afstand ongevraagd desinfecteren van een klantmachine.
Opzeggen overeenkomst	Het opzeggen van een internetovereenkomst met een klant na meerdere botnetinfecties.
Blokkeren van website	Het actief blokkeren van websites waardoor klanten kunnen worden geïnfecteerd.

Op de vraag wat effectief is in de strijd tegen botnets wordt door de verschillende partijen aangegeven dat educatie van de klant een belangrijk onderdeel is in de strijd tegen botnets.

Vervolgens is er nog gekeken op welk onderdeel van een botnet ISP's zich richten. Op basis van de interviews kan gesteld worden dat ISP's zich met name richten op de specifieke bots actief in hun eigen netwerk.

5.3 Het definitieve referentiemodel

5.3.1 Benodigde aanpassingen

Het theoretische referentiemodel, dat is opgesteld naar aanleiding van het literatuuronderzoek, is getoetst aan de empirie. Hieronder is per hoofdgebied aangegeven welke aanpassingen er zijn gedaan in het referentiemodel na toetsing aan de empirie.

5.3.1.1 Aanpassing preventie

Het referentiemodel is op de volgende punten aangepast:

- Door alle ISP's wordt aangegeven dat er met betrekking tot het klantverkeer geen gebruik gemaakt wordt van zogenaamde Intriusion Prevention Systems of Intrusion Detection Systems. Er zijn echter wel ISP's die dit als mogelijk commercieel product willen aanbieden of plannen hebben om dit te gaan aanbieden. De informatie met betrekking tot (mogelijke) besmettingen komt vanuit externe systemen. De ISP's worden derhalve extern gevoed over mogelijke besmettingen. Naar aanleiding van bovenstaande is er voor gekozen om de aspecten P-5 en D-8 uit Tabel 22 niet op te nemen in het definitieve referentiemodel.
- Het aspect P-6 uit Tabel 22 is gearceerd in het definitieve referentiemodel. Door twee van de vijf ISP's is aangegeven dat het nemen van (preventieve) technische maatregelen tegen botnets niet gebeurt en een derde ISP gaf aan dat dit beperkt plaatsvindt. Het nemen van technische maatregelen kan echter bijdragen aan het bestrijden van botnets door ISP's.
- Het aspect P-9 uit Tabel 22 met betrekking tot het abuse team is verplaatst in het referentiemodel van preventie naar detectie, omdat het abuse team pas in actie komt na een detectie. In Tabel 24 is dit aspect genummerd als D-9.
- Het aspect P-10 uit Tabel 22 is gearceerd in het definitieve referentiemodel, omdat het merendeel van de ISP's aangeeft geen gebruik te maken van Service Level Agreements met betrekking tot botnetbestrijding. Het opstellen van Service Level Agreements kan bijdragen aan betere procedures rond botnetbestrijding door ISP's.

- Het aspect P-11 uit Tabel 22 is gearceerd in het definitieve referentiemodel, omdat drie van de vijf ISP's op dit moment geen (of beperkt) standaardisering met betrekking tot botnets toepassen. Echter, standaardisering kan bijdragen aan het beter bestrijden van botnets door ISP's.

5.3.1.2 Aanpassing Detectie

Het referentiemodel is op de volgende punten aangepast:

- Het apsect D-1 uit Tabel 22 is gearceerd in het definitieve referentiemodel, omdat door ISP's wordt aangegeven dat dit niet of beperkt wordt gedaan met betrekking tot detectie van botnets.
- Het aspect D-2 uit Tabel 22 is gearceerd in het definitieve referentiemodel, omdat door de meerderheid van de ISP's is aangegeven dat er geen informatie van klanten wordt ontvangen over mogelijke besmettingen.
- Het aspect D-3 uit Tabel 22 is gearceerd in het definitieve referentiemodel, omdat het merendeel van de ISP's aangeeft niet of beperkt te communiceren over gedetecteerde besmettingen.
- Het aspect D-6 uit Tabel 22 is gearceerd in het definitieve referentiemodel, omdat de meeste ISP's geen Honeynet gebruiken voor detectie in hun netwerk.
- Het aspect D-8 uit Tabel 22 is verwijderd uit het definitieve referentiemodel, omdat door alle partijen wordt aangegeven dat dit niet wordt gedaan (zie uitleg preventie).
- Het aspect D-9 'abuse team' is toegevoegd aan het definitieve referentiemodel onder het onderdeel detectie.

5.3.1.3 Aanpassing notificatie

Het referentiemodel is op de volgende punten aangepast:

- Het aspect N-3 uit Tabel 22 is gearceerd in het definitieve referentiemodel, omdat drie van de vijf ISP's geen melding doen aan andere providers inzake botnets. Om botnetbestrijding goed te laten plaatsvinden, kan het doen van een melding inzake een botnetbesmetting aan een andere provider bijdragen aan het beter mitigeren van botnets.
- Het aspect N-4 uit Tabel 22 is verwijderd uit het referentiemodel, omdat botnetinfecties niet vallen onder de meldplicht datalekken.

5.3.1.4 Aanpassing verwijdering/bestrijding

Het referentiemodel is op de volgende punten aangepast:

- Het aspect V-3 uit Tabel 22 is gearceerd in het definitieve referentiemodel, omdat drie van de vijf ISP's dit niet toepassen in de strijd tegen botnets.
- Het aspect V-5 uit Tabel 22 is gearceerd in het definitieve referentiemodel, omdat door drie van de vijf ISP's geen informatie over verwijdering wordt gedeeld.

5.3.1.5 Aanpassing herstel

Het referentiemodel is op de volgende punten aangepast:

- Het aspect H-2 uit Tabel 22 is gearceerd in het definitieve referentiemodel, omdat drie van de vijf ISP's klanten niet of beperkt ondersteunen in het herstel na een botnetbesmetting.
- Het aspect H-4 uit Tabel 22 is gearceerd in het definitieve referentiemodel, omdat de meeste ISP's de klanten niet informeren over herstel na een botnetbesmetting.

5.3.2 Definitieve versie referentiemodel

In Tabel 24 is het definitieve referentiemodel opgenomen. Na de analyse van de empirische onderzoeksresultaten is het model geoptimaliseerd. De gedane aanpassingen zijn beschreven in paragraaf 5.3.1.

Tabel 24 Definitief referentiemodel

Preventie						
Doelgroep	Aspect	Naam kenmerk	Omschrijving	Technisch	Organisatorisch	Juridisch
Klant	P-1	Beschikbaar stellen end-point security	ISP's stellen end-point security oplossingen beschikbaar voor hun klanten. Dit kan bijvoorbeeld door klanten een antivirussoftware aan te bieden of een router met beveiliging.	x	x	
	P-2	Educatie van klanten	Door ISP's wordt er actief uitleg gegeven over het gevaar van botnets en de acties die klanten kunnen ondernemen om dit te voorkomen. Hierbij valt te denken aan: waarom klanten hun software up-to-date moeten houden, bewustwording campagnes, aanmoedigen van klanten om een end-point security oplossing te gebruiken, belang van backups en acties die klanten kunnen ondernemen om niet onderdeel te worden van een botnet. Eén van de doelen van educatie van klanten is de volgende: dat er bij de klant bewustwording ontstaat dat hij mede verantwoordelijk is in het voorkomen van een botnetbesmetting (gedeelde verantwoordelijkheid).	x	x	x
Andere partijen	P-3	Delen/communiceren van informatie/procedures omtrent botnetbestrijding	Door ISP's wordt er actief gecommuniceerd met andere stakeholders. Door ISP's wordt bijvoorbeeld informatie gedeeld met andere stakeholders over lessons-learned en procedures inzake botnetbestrijding.		x	
	P-4	Deelnemen in een samenwerkingsverband inzake botnetbestrijding	Door ISP's wordt actief deelgenomen in samenwerkingsverbanden met betrekking tot botnetbestrijding.		x	
ISP intern	P-6	Nemen van technische maatregelen inzake botnets	ISP's kunnen een aantal technische maatregelen nemen zodat het moeilijker wordt voor een botnet om machines te infecteren. Bijvoorbeeld het beveiligen van DNS servers.	x		
	P-7	Bijhouden stand van zaken met betrekking	ISP's blijven op de hoogte van de laatste ontwikkelingen met betrekking tot botnets en malware. Bijvoorbeeld door het trainen van	x	x	

		tot botnet/malware technieken.	personeel met betrekking tot bestrijding en detectie van botnets.			
	P-8	Klant support processen	Door de ISP's zijn er processen ingericht omtrent klantondersteuning inzake botnetbesmettingen.		x	
	P-10	Service Level Agreements	ISP's richten Service Level Agreements in met betrekking tot botnetbestrijding.		x	
	P-11	Standaardisering	Voldoen aan internationale standaarden inzake beveiliging (ISO 27002:2005, ISO 27006:2007)		x	
Detectie						
Klant	D-1	Aanbieden self-identify portal	Gebruikers zelf via tools, web portal of andere resource een mogelijke infectie laten vaststellen		x	
	D-2	Ontvangen informatie over mogelijke besmettingen via klanten	ISP's kunnen van klanten informatie krijgen over besmettingen binnen hun netwerk.		x	
Andere partijen	D-3	Communiceren gedetecteerde besmettingen	ISP's delen informatie over gedetecteerde besmettingen met andere ISP's.		x	
	D-4	Ontvangen informatie over mogelijke besmettingen via externe partijen	ISP's kunnen informatie over kwaadaardige activiteiten en bot geïnfecteerde klanten krijgen van externe partijen.		x	
	D-5	Ontvangen informatie over mogelijke besmettingen via AbuseHUB	ISP's ontvangen informatie over mogelijke besmettingen vanuit het AbuseHUB systeem.		x	
ISP intern	D-6	Honeynet	ISP's maken gebruik van honeypots om besmettingen in het netwerk te kunnen constateren.	x		
	D-7	Detectie besmetting	Als een besmetting wordt geconstateerd, of daarop wordt gewezen door een derde, zal de ISP binnen een redelijke termijn beoordelen of hij hier tegen moet optreden.	x		
	D-9	Abuse team	ISP's hebben een abuse team actief.		x	
Notificatie						
Klant	N-1	Melding aan geïnfecteerde klanten	Gebruiker informeren over een mogelijke besmetting Dit kan via email, telefoon, in-browser, instantmessaging, SMS of via walled garden bericht.		x	
	N-2	Koppeling melding met remediation tools	De melding die de gebruiker in geval van besmetting ontvangt, bevat ook informatie over tools en middelen om het probleem op te lossen.	x	x	
Andere partijen	N-3	Melding aan andere providers	ISP's melden besmettingen aan andere providers.		x	
Verwijdering/bestrijding						
Klant	V-1	Isoleren gebruiker	Het plaatsen van geïnfecteerde gebruikers in een zogenaamde 'walled garden'.	x	x	
	V-2	Delen van informatie omtrent het oplossen van een botnetinfectie	ISP's stellen informatie beschikbaar hoe klanten een mogelijke botnetinfectie kunnen oplossen.	x	x	
	V-3	Links naar professionele hulp	De ISP kan klanten informatie geven over waar de klant professionele hulp kan vragen.		x	
Klant / Andere partijen	V-4	Delen procedure walled garden	De procedure rond het isoleren van besmettingen (walled garden) wordt gedeeld met klanten en andere ISP's zodat voor klanten duidelijk is wanneer zij weer gebruik van hun verbinding kunnen maken.		x	

Andere partijen	V-5	Delen best practices verwijdering	ISP's delen informatie met betrekking tot het verwijderen van botnets met andere instanties.		x	
Herstel						
Klant	H-1	Activeren verbinding klant	De ISP bepaalt op welk moment en hoe een consument weer gebruik kan maken van de internetverbinding nadat de besmetting is verwijderd.	x	x	
	H-2	Ondersteunen van klanten in herstel	ISP's stellen informatie over remediation beschikbaar (dit kan via publicaties of web links) over hoe een klant een botnetinfectie kan oplossen.		x	
	H-3	Gevolgen herstel met betrekking tot persoonlijke data en accounts	De ISP informeert de klant welke gevolgen het oplossen van een besmetting heeft met betrekking tot persoonlijke bestanden.		x	
	H-4	Informatie herstel	ISP's stellen informatie beschikbaar die klanten kunnen helpen in het herstellen van hun data na het oplossen van een botnetbesmetting.		x	

De gearceerde onderdelen in Tabel 24 worden niet door alle ISP's toegepast. Echter, de gearceerde onderdelen kunnen wel bijdragen aan het beter mitigeren van botnets. Het opgestelde definitieve referentiemodel kan derhalve worden gebruikt om te inventariseren waar ISP's nog actie moeten ondernemen.

6 Conclusies en aanbevelingen

In dit hoofdstuk worden de conclusies en aanbevelingen van het afstudeeronderzoek gepresenteerd. Het onderzoek is uitgevoerd in een theoretisch deel en in een empirisch deel. In de onderstaande paragrafen wordt eerst teruggeblikt op de beantwoording van de verschillende onderzoeksvragen om vervolgens de hoofdvraag van het onderzoek te beantwoorden.

6.1 Conclusie literatuuronderzoek

Als algehele conclusie voor het literatuuronderzoek kan het volgende worden gesteld.
Botnets zijn een grote cyberbedreiging voor onze maatschappij. Botnets kunnen door cybercriminelen om allerlei redenen/motieven worden ingezet. ISP's kunnen een belangrijke bedrage leveren aan de botnetbestrijding. Deze bijdragen kunnen zij volgens de anti-botnet life cycle in vijf hoofdgebieden leveren. Echter, is er wel een beperking aan te brengen dat niet alle voorstellen, die in recente literatuur worden gedaan met betrekking tot botnetbestrijding, zomaar door ISP's kunnen worden toegepast. Aan deze voorstellen kleven juridische beperkingen. Anderzijds hebben ISP's een zorgplicht richting hun klant.

Daarnaast is er gekeken naar samenwerkingsinitiatieven met betrekking tot botnetbestrijding. Binnen Nederland is de verenging Abuse Information Exchange actief. Binnen deze verenging is 90 procent van de Nederlandse ISP's actief. Door de verenging is er een systeem actief dat de leden van informatie voorziet met betrekking tot besmette apparaten in hun netwerk. Echter, zijn er nog geen resultaten bekend van de werking van het systeem met betrekking tot botnetbestrijding.

In totaal zijn er zeven onderzoeksvragen gesteld tijdens het literatuuronderzoek. Hieronder worden ze allen beknopt behandeld.

Wat zijn botnets?
Botnets zijn netwerken van samenwerkende apparaten die zijn geïnfecteerd (onvrijwillig) met (dezelfde) malware en onder controle staan van een persoon of organisatie en gecoördineerd cyberaanvallen kunnen uitvoeren.

Hoe hebben botnets zich de afgelopen jaren geëvolueerd/ontwikkeld en welke gevolgen heeft dit?
Botnets evolueren continue. Er worden nog steeds nieuwe technieken ontdekt die botnetontwikkelaars toepassen. Er is sprake van een zogenaamd kat en muis spel tussen aan de ene kant de botnet ontwikkelaars/operators en aan de andere kant de security experts.
Op dit moment voeren de cybercriminelen/botnetontwikkelaars de boventoon.

Hoe vindt de bestrijding van botnets plaats vanuit technisch oogpunt, organisatorisch oogpunt en juridisch oogpunt

In de literatuur zijn verschillende technieken te vinden om botnets te detecteren. Grofweg kan het detecteren van botnets worden opgedeeld in honeynet-based en Intrusion Detection System (IDS). Nadat een botnet is gedetecteerd kunnen er tegenmaatregelen worden genomen. Deze tegenmaatregelen kunnen zich richten op de verschillende onderdelen van een botnet. Er zijn verschillende technische maatregelen te nemen tegen botnets. Bij meerdere technische maatregelen kunnen op juridisch vlak beperkingen optreden. Om succesvol te zijn in de strijd tegen botnets is samenwerking van essentieel belang. Bij het ontmantelen van een botnet zijn vaak meerdere organisaties betrokken.

Wat kunnen Internet Service Providers bijdragen in de bestrijding van botnets?

Volgens meerdere studies wordt een centrale rol toegedicht aan ISP's in de strijd tegen botnets. De mate waarin ISP's actie ondernemen tegen botnets is niet of nauwelijks beschreven in de literatuur. Echter, er zijn allerlei documenten van verschillende organisatie en samenwerkingsverbanden te vinden met daarin zogenaamde best practices wat ISP's kunnen doen tegen botnets. Botnetbestrijding door ISP's kan plaatsvinden volgens de zogenaamde anti-botnet life cycle. In de anti-botnet life cycle worden de volgende vijf gebieden beschreven: preventie, detectie, notificatie, verwijdering/bestrijden en herstel. Uit de verzamelde literatuur zijn de aanbevelingen, die ISP's kunnen ondernemen tegen botnets, gegroepeerd en waar nodig samengevoegd en toegewezen aan één van deze vijf gebieden.

Welke juridische verantwoordelijkheden (rechten en plichten) hebben Internet Service Providers in relatie tot botnetbestrijding?

Het is onduidelijk wat ISP's moeten doen in het geval van ontdekking van een botnet binnen hun netwerk. Het ontbreekt op dit moment aan een juridisch kader voor ISP's om botnets verplicht aan te pakken. Gesteld kan worden dat de acties die ISP's ondernemen inzake botnetbestrijding op vrijwillige basis plaatsvinden. Echter, er rust op de ISP's wel een zogenaamde zorgplicht richting de klant. ISP's zijn verplicht om technische en organisatorische maatregelen te treffen ter bescherming tegen internetcriminaliteit. Verder dienen ISP's er voor te zorgen dat zij voldoende informatie aan hun abonnees ter beschikking stellen, zodat die een inschatting kunnen maken van de risico's die ze lopen door gebruik te maken van de internetdiensten van de ISP. Op de ISP's rusten dus inspanningsverplichtingen van technische, organisatorische en informatieve aard.

Wat doen Internet Service Providers afzonderlijk van elkaar aan botnetbestrijding?

In de literatuur is niet terug te vinden wat de individuele ISP doet aan botnetbestrijding. Daarnaast zijn er nagenoeg geen cijfers bekend inzake het aantal klanten dat besmet wordt per ISP per jaar. De meeste providers hebben een abuse afdeling actief waar klanten terecht kunnen in geval van een besmetting. De meeste providers kunnen bij misbruik van een verbinding van een klant de klant isoleren in een zogenaamde walled garden omgeving.

Welke samenwerkingsinitiatieven zijn er te vinden over hoe Internet Service Providers samenwerken met andere partijen met betrekking tot botnetbestrijding?
In de literatuur zijn er verschillende samenwerkingsverbanden terug te vinden. Sommige samenwerkingsverbanden opereren wereldwijd. Binnen Nederland is de Verenging Abuse Information Exchange actief. De verenging heeft een zogenaamd clearing house opgezet, genaamd AbuseHub. De AbuseHub levert informatie over besmettingen aan de aangesloten leden.

6.2 Conclusies empirisch onderzoek

Als algehele conclusie voor het empirisch onderzoek kan gesteld worden dat de verschillende benaderde partijen zich kunnen vinden in het opgestelde referentiemodel. Na input van de verschillende partijen is het referentiemodel herzien. Bij de verschillende geïnterviewde partijen is aandacht voor het probleem van botnets.

Na het uitvoeren van de verschillende interviews kunnen per onderzoeksvraag verschillende conclusies worden getrokken. Hieronder is per onderzoeksvraag een conclusie gegeven naar aanleiding van de verschillende interviews.

Wat wordt door ISP's verstaan onder botnets?
Door de ondervraagde partijen wordt nagenoeg één en dezelfde definitie gehanteerd. Op een aantal kleine punten is er verschil in bewoording.

Hoe worden botnets geclassificeerd door ISP's?
De onderzoeksvraag met betrekking tot classificatie is verschillend beantwoord. Sommige ISP's hanteren geen classificatie voor een botnet nadat deze is gedetecteerd. Andere ISP's hanteren een eenvoudige benadering in classificatie. De classificatie op commandostructuur zoals deze voorkomt in de literatuur is niet waargenomen tijdens het empirisch onderzoek.

Aan welke samenwerkingsverbanden worden door ISP's deelgenomen?
Het merendeel van de ISP's neemt deel aan samenwerkingsverbanden in de strijd tegen botnets. Vier van de vijf ISP's nemen deel aan de Vereniging Abuse Information Exchange. De ISP's die hieraan deelnemen, ontvangen van deze vereniging informatie over mogelijke botnetbesmettingen.

Is het opgestelde theoretisch referentiemodel compleet?
Door de verschillende partijen wordt aangegeven dat het referentiemodel compleet is. Er is echter in het referentiemodel een aantal aspecten opgenomen die door de ISP's niet worden uitgevoerd of nog een wens voor de toekomst zijn.

Is het opgestelde theoretische referentiemodel correct?
Door de verschillende partijen wordt aangegeven dat het referentiemodel in hoofdlijnen correct is. Met de verschillende partijen is het referentiemodel doorlopen en zijn de opmerkingen verwerkt in de vraagverwerkingslijst.

6.3 Conclusie hoofdvraag

De centrale onderzoekvraag die in dit afstudeeronderzoek gesteld wordt, is de volgende:
'Welke rol spelen Internet Service Providers bij de bestrijding van botnets op technisch gebied, hoe pakken ze dit organisatorisch aan en wat zijn juridisch gezien de mogelijkheden en beperkingen?'

Na het uitvoeren van het onderzoek is het mogelijk om de centrale onderzoeksvraag te beantwoorden. Het definitieve referentiemodel geeft goed weer hoe ISP's gepositioneerd zijn in de bestrijding van botnets. Het definitieve referentiemodel laat zien wat ISP's doen in de strijd tegen botnets. Daarnaast is het referentiemodel opgedeeld in de verschillende fasen van de anti-botnet life cycle. Acties die ISP's kunnen ondernemen zijn technisch, organisatorisch of juridisch van aard. De ISP's zijn zich bewust van hun zorgplicht richting de klant. ISP's houden zich aan de afspraak die is gemaakt in het convenant van de werkgroep botnets om niet actief mee te kijken in het netwerkverkeer van de klant. Informatie over besmettingen komt niet door middel van actieve monitoring tot stand. ISP's richten zich in de meeste gevallen, als het gaat om botnetbestrijding, tot de individuele bots die actief zijn bij de klant.

6.4 Aanbevelingen voor vervolg onderzoek

Er wordt in de literatuur veel aandacht besteed aan de centrale rol die ISP's innemen in de strijd tegen botnets. In het in dit onderzoek opgeleverde referentiemodel zijn de aspecten die ISP's kunnen inzetten tegen botnets onderverdeeld in vijf hoofdgebieden. Door de verschillende geïnterviewde partijen wordt er veel waarde gehecht de volgende aspecten:

- P-1 Beschikbaar stellen end-point security;
- P-2 Educatie van klanten;
- P-4 Deelnemen in een samenwerkingsverband inzake botnetbestrijding.

Het is vanzelfsprekend interessant om verder te onderzoeken wat de invloed van deze aspecten is op botnetbestrijding door ISP's. Van bovengenoemde aspecten wordt immers veel verwacht in de strijd tegen botnets.

7 Reflectie

7.1 Productreflectie

Als onderzoeker ben je altijd op zoek naar iets waarmee je een bijdrage levert aan de wetenschap. Persoonlijk hoopte ik iets te vinden wat wereldschokkend is. Helaas is dit niet het geval. Echter, er is wel een beeld geschetst van de huidige stand van zaken met betrekking tot botnetbestrijding door ISP's. Het uiteindelijke referentiemodel geeft aan wat ISP's doen aan botnetbestrijding binnen Nederland.

Uiteindelijk zijn alle onderzoeksvragen beantwoord en hiermee kan ook de hoofdvraag worden beantwoord. Zoals altijd is er genoeg aanleiding tot een vervolgonderzoek.

7.2 Procesreflectie

Als er teruggeblikt wordt op het totale proces is er altijd een aantal verbeterpunten. Het totale traject heeft meer dan anderhalf jaar in beslag genomen. Eén van de punten waar ik mijzelf op kan verbeteren is het gestructureerd en planmatig werken. Meerdere keren tijdens de afstudeerperiode is de planning bijgesteld. Eén van de 'gelukkige' redenen om de planning bij te stellen was de geboorte van mijn tweede kind. Daarnaast was het aannemen van een andere functie binnen de organisatie misschien iets minder gelukkig getimed. Door het uitvoeren van een andere functie heeft het afstudeertraject enige vertraging opgelopen.

Een probleem voor het proces is de constante aandacht voor het onderwerp botnets. Met enige regelmaat verschijnen er nieuwe publicaties met betrekking tot het onderwerp. Tijdens het schrijven van het verslag heb ik mijzelf moet beheersen om toch geen nieuwe 'recentere' publicaties te gaan toevoegen.

8 Referenties

Wetenschappelijke literatuur

Abdullah, R. S., Abu, N. A., Faizal, M., & Noh, Z. A. M. (2014). Understanding the Threats of Botnets Detection: A Wide Scale Survey. *Research Journal of Information Technology, 6*(3), 135-153.

Asghari, H. (2010). *Botnet mitigation and the role of ISPs: A quantitative study into the role and incentives of Internet Service Providers in combating botnet propagation and activity.* TU Delft, Delft University of Technology.

Banday, M. T., Qadri, J. A., & Shah, N. A. (2009). Study of Botnets and their threats to Internet Security.

Cooke, E., Jahanian, F., & McPherson, D. (2005). *The zombie roundup: Understanding, detecting, and disrupting botnets.* Paper presented at the Proceedings of the USENIX SRUTI Workshop.

Czosseck, C., Klein, G., & Leder, F. (2011). *On the arms race around botnets-Setting up and taking down botnets.* Paper presented at the Cyber Conflict (ICCC), 2011 3rd International Conference on.

Edwards, L. (2011). The Role of Internet Intermediaries in Advancing Public Policy Objectives Forging Partnerships for Advancing Policy Objectives for the Internet Economy, Part II. *Part II (June 22, 2011)*.

Estrada, V. C., & Nakao, A. (2010). *A survey on the use of traffic traces to battle internet threats.* Paper presented at the Knowledge Discovery and Data Mining, 2010. WKDD'10. Third International Conference on.

Feily, M., Shahrestani, A., & Ramadass, S. (2009). *A survey of botnet and botnet detection.* Paper presented at the Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on.

Grizzard, J. B., Sharma, V., Nunnery, C., Kang, B. B., & Dagon, D. (2007). *Peer-to-peer botnets: Overview and case study.* Paper presented at the Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets.

Khattak, S., Ramay, N. R., Khan, K. R., Syed, A. A., & Khayam, S. A. (2014). A taxonomy of botnet behavior, detection, and defense. *Communications Surveys & Tutorials, IEEE, 16*(2), 898-924.

Kim, W., Jeong, O.-R., Kim, C., & So, J. (2010). *On botnets.* Paper presented at the Proceedings of the 12th International Conference on Information Integration and Web-based Applications & Services.

Leder, F., Werner, T., & Martini, P. (2009). Proactive botnet countermeasures: an offensive approach. *The Virtual Battlefield: Perspectives on Cyber Warfare, 3*, 211-225.

Li, C., Jiang, W., & Zou, X. (2009). *Botnet: Survey and case study.* Paper presented at the Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on.

Marshall, C., & Rossman, G. (1999). Designing qualitative research . 1999: Thousand Oaks, CA: Sage Publications.

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *The Journal of Economic Perspectives, 23*(3), 3-20.

Oecd. (2012). Proactive Policy Measures by Internet Service Providers against Botnets. Retrieved from http://EconPapers.repec.org/RePEc:oec:stiaab:199-en

OpenDNS. (2011). The Role of DNS in Botnet Command & Control.

Plohmann, D., Gerhards-Padilla, E., & Leder, F. (2011). Botnets: Detection, measurement, disinfection & defence. *The European Network and Information Security Agency (ENISA)*.

Robson, C. (2002). *Real world research* (Vol. 2): Blackwell publishers Oxford.

Rodríguez-Gómez, R. A., Maciá-Fernández, G., & García-Teodoro, P. (2013). Survey and taxonomy of botnet research through life-cycle. *ACM Computing Surveys (CSUR), 45*(4), 45.

Salemink, K., & Strijker, D. (2012). Breedband op het platteland. Rapportage voor Woon-en Leefbaarheidsbasisplan Oost-Groningen.

Schless, T. (2013). De organisatie van botnetbestrijding in Nederland.
Shin, S., Lin, R., & Gu, G. (2011). *Cross-analysis of botnet victims: New insights and implications.* Paper presented at the Recent Advances in Intrusion Detection.
Silva, S. S., Silva, R. M., Pinto, R. C., & Salles, R. M. (2013). Botnets: A survey. *Computer Networks, 57*(2), 378-403.
Tiirmaa-Klaar, H., Gassen, J., Gerhards-Padilla, E., & Martini, P. (2013). Botnets, Cybercrime and National Security *Botnets* (pp. 1-40): Springer.
van Eeten, M. J. G., Asghari, H., Bauer, J., & Tabatabaie, S. (2011). Internet service providers and botnet mitigation: A fact-finding study on the Dutch market. *Delft University of Technology*.
van Eeten, M. J. G., & Bauer, J. M. (2008). Economics of malware: Security decisions, incentives and externalities.
van Eeten, M. J. G., Bauer, J. M., Asghari, H., & Tabatabaie, S. (2010). *The role of internet service providers in botnet mitigation an empirical analysis based on spam data*.
van Eeten, M. J. G., Lone, Q., & Moura, G. C. (2014). Towards Incentivizing ISPs to Mitigate Botnets *Monitoring and Securing Virtualized Networks and Services* (pp. 57-62): Springer.
Verschuren, P. J. M., & Doorewaard, H. (2007). *Het ontwerpen van een onderzoek*: Lemma.
Wang, P., Sparks, S., & Zou, C. C. (2010). An advanced hybrid peer-to-peer botnet. *Dependable and Secure Computing, IEEE Transactions on, 7*(2), 113-127.
Wang, T., Wang, H., Liu, B., & Shi, P. (2013). *What is the Pattern of a Botnet?* Paper presented at the Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on.
Zeidanloo, H. R., & Manaf, A. A. (2009). *Botnet command and control mechanisms.* Paper presented at the Computer and Electrical Engineering, 2009. ICCEE'09. Second International Conference on.

Niet-wetenschappelijke bronnen

Australian Communications and Media Authority. (2014). ACMA fights malware on two fronts. Geraadpleegd op 16 maart 2015, via http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/acma-fights-malware-on-two-fronts
Autoriteit Consument & Markt [ACM]. (2014). Telecommonitor tweede kwartaal 2014. Geraadpleegd op 15 december 2014, via https://www.acm.nl/nl/download/publicatie/?id=13552
Business Insider. (2013). Here's Why 'The Internet Of Things' Will Be Huge, And Drive Tremendous Value For People And Businesses. Geraadpleegd via http://www.businessinsider.com/growth-in-the-internet-of-things-2013-10?IR=T
Centraal Bureau voor de Statistiek. (2014). ICT kennis en economie 2014. Geraadpleegd via http://www.cbs.nl/NR/rdonlyres/4DEFB273-9BC7-459B-8788-44C94175DA4B/0/2014i78pub.pdf
Centraal Bureau voor de Statistiek [CBS]. (2013). ICT gebruik van huishoudens naar huishoudkenmerken. Geraadpleegd op 4 januari 2015, via http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=71102ned&D1=a&D2=0-5&D3=a&VW=T
CNET. (2014). Fridge caught sending spam emails in botnet attack. Geraadpleegd op 15 december 2014, via http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/
Communications Alliance. (2014). C650:2014 iCode. Geraadpleegd op 16 maart 2015, via http://www.commsalliance.com.au/Documents/all/codes/icode
CSRIC. (2010). Internet Service Provider (ISP) Network Protection Practices. Geraadpleegd via https://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf
ECP. (2009). Raamwerk afspraken botnetbestrijding. Geraadpleegd via https://ecp.nl/bijlagen/3889/raamwerk-afspraken-botnetbestijding-definitief.pdf
ECP. (2015). Jaarverslag 2014 - 2015. Geraadpleegd via http://ecp.onlineblad.nl/#Cover

Europol. (2015). Botnet taken down through international law enforcement cooperation. Geraadpleegd op 1 maart 2015, via https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation

Houthoff Buruma. (2013). Privacy: Tips & Tricks voor de Ondernemingspraktijk, . Geraadpleegd via http://www.houthoff.com/uploads/tx_hhpublications/Privacy_boek.pdf

Internet Industry Association. (2014). Internet Service Providers Voluntary Code of Practice. Geraadpleegd via http://www.commsalliance.com.au/__data/assets/pdf_file/0019/44632/C650_2014.pdf

Jacobs, B. (2013). De DDoS paradox: Ontsluiten door afsluiten. Geraadpleegd via http://www.cs.ru.nl/B.Jacobs/PAPERS/NJB-2013-32-Focus-Jacobs.pdf

Koops, B. J. (2013). Acties tegen botnets door SURFnet en bij SURFnet aangesloten instellingen: strafrechtelijke aspecten. Geraadpleegd op 10 december 2014, via https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/expert_opinion_botnets_koops_mei_2013.pdf

Koops, B. J., & van der Hof, S. (2002). Informatiebeveiliging, e-handel en recht. Geraadpleegd via https://pure.uvt.nl/ws/files/484472/informatiebeveiliging.pdf

Leenes, R. (2013). Acties tegen botnets door SURFnet en bij SURFnet aangesloten instellingen: privacy & data protectie aspecten. Geraadpleegd via https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/expert_opinion_botnets_leenes_oktober_2013.pdf

Livingood, J., & Mody, N. (2012). Recommendations for the Remediation of Bots in ISP Networks.

Messaging Malware and Mobile Anti-Abuse Working Group. (2015). M3AAWG Best Common Practices for the Use of a Walled Garden.

Ministerie van Veiligheid en Justitie. (2013). Opstelten versterkt aanpak computercriminaliteit. Geraadpleegd op 8 maart 2015, via https://www.rijksoverheid.nl/actueel/nieuws/2013/05/02/opstelten-versterkt-aanpak-computercriminaliteit

Nationaal Cyber Security Centrum. (2012). Cybersecuritybeeld Nederland CSBN-2. Geraadpleegd via https://www.nctv.nl/Images/ncsc-cybersecuritybeeld-nederland_tcm126-444007.pdf

Nationaal Cyber Security Centrum. (2013). Cybersecuritybeeld Nederland CSBN-3. Geraadpleegd via https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland-3.html

Nationaal Cyber Security Centrum. (2014). Cybersecuritybeeld Nederland CSBN-4. Geraadpleegd via https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-4/1/CSBN%2B4.pdf

Online Trust Alliance. (2012). Combatting Botnets Through User Notification Across the Ecosystem. Geraadpleegd via https://otalliance.org/system/files/files/best-practices/documents/ota_botnet_notification_whitepaper12-7.pdf

Online Trust Alliance. (2013). Botnet Remediation Overview & Practices. Geraadpleegd via Botnet Remediation Overview & Practices

Opstelten, I. W. (2014). Kamerbrief Aanpak van botnets. Geraadpleegd op 15-10-2014, via http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/07/08/aanpak-van-botnets.html

Saunders, M., Lewis, P., & Thornhill, A. (2011). *Methoden en technieken van onderzoek* (De 5e editie ed.). Amsterdam: Pearson Education Benelux.

Security.NL. (2014). Australische overheid toont isp's besmette abonnees. Geraadpleegd op 15 januari 2015, via https://www.security.nl/posting/410151/Australische+overheid+toont+isp%27s+besmette+abonnees

SURFnet. (2013). SURFnet ontwikkelt gedragscodes rondom anti-botnetacties. Geraadpleegd via https://www.surf.nl/nieuws/2013/11/surfnet-ontwikkelt-gedragscodes-rondom-anti-botnetacties.html

SURFnet. (2015). Aangesloten instellingen. Geraadpleegd op 16 maart 2015, via https://www.surf.nl/over-surf/werkmaatschappijen/surfnet/over-surfnet/aansluiten-op-surfnet/aangesloten-instellingen/index.html

Van Eeckhoutte, F. J. (2010). Zorgverplichtingen ISP's tegen internetcriminaliteit Geraadpleegd via http://www.vaneeckhoutteadvocaten.nl/ArtZorgverplichtingenIspsTegenInternetcriminaliteit01.html

Vereniging Abuse Information Exchange. (2013). Abuse Information Exchange AbuseHUB. Geraadpleegd via http://jaarcongresecp.nl/uploads/bestanden/2013/Abuse_Information_Exchange.pdf

Vereniging Abuse Information Exchange (2014). Abuse Information Exchange. Geraadpleegd op 16 maart 2015, via https://www.abuseinformationexchange.nl/

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*: Crown.

Bijlagen

Bijlage 1: Uitnodigingsemail Internet Service Providers

Hallo meneer …,

Mijn naam is Jeroen Pijpker en ik ben werkzaam voor de Stenden hogeschool in Emmen als docent/teamleider bij de opleiding Informatica. Naast mijn werk voor de hogeschool volg ik een studie bij de Open Universiteit. Ik ben op dit moment bezig met mijn afstudeeronderzoek voor de opleiding Business Process Management & IT van de Open Universiteit. Het afstudeeronderzoek heeft als titel '***De rol van Internet Service Providers bij de bestrijding van botnets'***.

Voor dit afstudeeronderzoek heb ik eerst een literatuurstudie uitgevoerd waaruit een (theoretisch) referentiemodel is ontstaan dat weergeeft hoe Internet Service Providers volgens de literatuur botnets bestrijden. Dit model zou ik graag met u willen evalueren middels een interview.

Door het zoeken via internet naar bijvoorbeeld security officers en de naam van een Internet Service Provider (onder andere via LinkedIn) ben ik uw naam en emailadres tegengekomen. Voor dit onderzoek lijkt het mij belangrijk om de input van … te verwerken in het onderzoek, omdat … lid is van de Vereniging Abuse Information Exchange. Daarom hoop ik op uw medewerking.

Ik zou graag een interview bij u willen afnemen waarin we het referentiemodel, hoe Internet Service Providers botnets bestrijden, met elkaar bespreken. Ik zou graag een afspraak met u maken. Mijn voorkeur gaat uit naar face-to-face, maar als dit niet mogelijk is, kan het telefonisch of via Skype. Voorafgaand aan het interview zal ik dan achtergrondinformatie en de interviewvragen naar u emailen.

Onderaan deze email staan mijn contactgegevens. Natuurlijk worden alle onderzoeksresultaten vertrouwelijk behandeld en zullen de resultaten geanonimiseerd worden. Wel zou ik een verslag of een presentatie voor uw team kunnen geven (nadat alle onderzoeken zijn afgerond).

Ik hoop dat u wilt meewerken aan mijn onderzoek.

Met vriendelijke groet,

Jeroen Pijpker

Telefoonnummer: 06-20863195
Emailadres: jeroen.pijpker@stenden.com

Bijlage 2: Toestemmingsformulier

Toestemmingsformulier

Titel van het onderzoeksproject:
De rol van Internet Service Providers bij de bestrijding van botnets

Naam en functie onderzoeker:
Jeroen Pijpker, teamleider Informatica Stenden hogeschool, Master BPMIT, Open Universiteit Nederland

	Zet uw paraaf in het vakje ja	nee
1. Ik begrijp dat mijn deelname vrijwillig is en dat ik deze op elk moment kan beëindigen zonder opgaaf van reden.	☐	☐
2. Ik ben mij ervan bewust dat, hoewel alles in het werk gesteld zal worden om de vertrouwelijkheid te waarborgen van de informatie die ik geef, dit alleen binnen de grenzen van de wet kan worden gegarandeerd.	☐	☐
3. Ik stem toe deel te nemen aan dit onderzoek.	☐	☐
4. Ik geef toestemming om in publicaties anonieme citaten te gebruiken.	☐	☐

Naam van de deelnemer: Datum: Handtekening:

Jeroen Pijpker (onderzoeker): Datum:
Handtekening:

Bijlage 3: Verstrekte informatie interviewkandidaten

Inleiding afstudeeronderzoek

In meerdere onderzoeken wordt aangegeven dat botnets één van de grootste bedreigingen zijn op het internet. In het Cybersecuritybeeld van 2013 voor Nederland wordt aangegeven dat botnets de grootste cyberbedreiging vormen in Nederland. In het daarop volgende Cybersecuritybeeld van 2014 wordt aangegeven dat het gebruik van botnets winstgevender wordt voor de cybercriminelen en dat botnets steeds beter worden verhuld en verdedigd (Nationaal Cyber Security Centrum, 2013).

Bij de bestrijding van botnets zijn private en publieke organisaties betrokken. Een belangrijke private partij bij de bestrijding van botnets zijn de Internet Service Providers (ISP). De traditionele rol van ISP's is het voorzien van klanten van internettoegang en het verkeer van de klanten te behandelen volgens de netneutraliteitrichtlijnen. In verschillende onderzoeken wordt gesteld dat ISP's een centrale rol kunnen spelen bij het bestrijden van botnets.

Daarnaast worden in de theorie allerlei maatregelen en best practices genoemd die ISP's kunnen toepassen in de strijd tegen botnets.

Dit afstudeeronderzoek levert een theoretische bijdrage aan het aspect botnetbestrijding door te onderzoeken welke rol ISP's spelen bij botnetbestrijding. Het afstudeeronderzoek wil inzicht geven in wat ISP's kunnen doen aan botnetbestrijding, wat mogen ISP's wel en niet en hoe staat dit in verhouding tot de juridische bevoegdheden.

Probleemstelling

De algemene hoofdvraag van het afstudeeronderzoek is de volgende:
'Welke rol spelen Internet Service Providers bij de bestrijding van botnets op het technisch gebied, hoe pakken ze dit organisatorisch aan en wat zijn juridisch gezien de mogelijkheden en beperkingen?'

De doelstelling van het afstudeeronderzoek:
'***Het doel van het afstudeeronderzoek is vaststellen welke rol Internet Services Providers op dit moment spelen bij de bestrijding van botnets in Nederland.***'

Op basis van het literatuuronderzoek is een referentiemodel opgesteld die weergeeft hoe ISP's botnetbestrijding hebben vormgegeven. Het referentiemodel is opgedeeld in vijf verschillende hoofdgebieden die zijn ontleend aan de anti-botnet life cycle (zie figuur 1). Deze vijf gebieden zijn:

- Preventie (prevention) - proactieve maatregelen/activiteiten vanuit de ISP om te voorkomen dat een device geïnfecteerd raakt.
- Detectie (detection) – maatregelen/activiteiten met als doel het identificeren van bedreigingen op het netwerk van bijvoorbeeld een ISP.

- Notificatie (notification) – maatregelen/activiteiten die worden ondernomen om gebruiker of verantwoordelijke te informeren.
- Verwijdering/bestrijding (remediation) – maatregelen/activiteiten die worden ondernomen om malware te verwijderen van een geïnfecteerd device.
- Herstel (recovery) – maatregelen/activiteiten die worden ondernomen om de impact van een aanval op te lossen.

Figuur 1 Anti-botnet life cycle

Het opgestelde theoretisch referentiemodel is als bijlage toegevoegd.

Voor het beantwoorden van de hoofdvraag van het afstudeeronderzoek zijn de volgende onderzoeksvragen geformuleerd die door middel van interviews zullen worden beantwoord:

- Wat wordt door ISP's verstaan onder botnets?
- Hoe worden botnets geclassificeerd door ISP's?
- Aan welke samenwerkingsverbanden worden door ISP's deelgenomen (op nationaal, Europees en wereldwijd niveau)?
- Is het opgestelde theoretisch referentiemodel compleet?
  Zijn er aspecten op het gebied van botnetbestrijding die niet voorkomen in het theoretisch referentiemodel, maar wel van toepassing zijn op de manier waarop botnetbestrijding wordt uitgevoerd door ISP's?
- Is het opgestelde theoretische referentiemodel correct?
  Zijn de aspecten die voorkomen in het theoretisch referentiemodel van toepassing op het juiste gebied (technisch, organisatorisch, juridisch)?

Opzet van het interview

Het interview bestaat uit een algemeen deel, vragen met betrekking tot het onderzoek en vragen gebaseerd op de empirische deelvragen.

1.1 Algemene vragen

1.1.1 Geïnterviewde
- Wat is uw naam (incl. voorletters, evt. titels)?
- Wat is uw functie/relatie tot botnetbestrijding?
- Wat zijn uw belangrijkste taken, verantwoordelijkheden en bevoegdheden?
- Voor welke Internet Service Provider werkt u?

1.1.2 Organisatie
- Wat is de naam van de organisatie waarvoor u werkt?
- Hoe is op hoofdlijnen de organisatie ingericht? Maakt de organisatie deel uit van een grotere organisatie?
- Zijn er openbare publicaties beschikbaar, zoals rapporten en jaarverslagen, van en over uw organisatie waarin cyber security in het algemeen of botnetbestrijding aan bod komt?

1.2 Samenwerkingsverbanden
- Bent u bekend met samenwerkingsverbanden op het gebied van botnetbestrijding?
- Welke samenwerkingsverbanden inzake botnetbestrijding kent u?
- Aan welke samenwerkingsverbanden neemt uw organisatie deel? Zo ja, is dit een samenwerkingsverband binnen Nederland, Europa of wereldwijd.

1.3 Botnets
In dit onderzoek is voor de volgende definitie gekozen voor botnets.
Botnets zijn netwerken van samenwerkende apparaten die zijn geïnfecteerd (onvrijwillig) met (dezelfde) malware en onder controle staan van een persoon of organisatie en gecoördineerd cyberaanvallen kunnen uitvoeren.

- Welke definitie wordt binnen uw organisatie gehanteerd voor botnets?
- Hoe worden botnets geclassificeerd?

1.4 Referentiemodel

Tijdens de literatuurstudie is er een referentiemodel (bijlage 1) ontwikkeld waarin is aangegeven hoe vanuit de literatuur botnetbestrijding door ISP's is vormgegeven.

1.4.1 Botnetbestrijding aspecten

In dit onderzoek is botnetbestrijding onderverdeeld in een 5-tal deelgebieden, namelijk:

- Preventie
- Detectie
- Notificatie
- Verwijdering
- Herstel

Vervolgens zijn er per deelgebied aspecten onderverdeeld die ISP's kunnen toepassen in de strijd tegen botnets. Deze aspecten kunnen van technische, organisatorisch of juridische aard zijn.

Voor elk van de aspecten uit het model worden de volgende vragen gesteld:

- Is dit aspect volgens u van toepassing voor uw organisatie?
- Is de classificatie van het aspect juist? Zo nee, waarom niet en welke classificatie(s) is of zijn volgens u van toepassing op het aspect?
- Is het aspect onderverdeeld in het juiste deelgebied? Zo nee, welk deelgebied is dan van toepassing en waarom?
- Is het aspect toegekend aan de juiste doelgroep? Zo nee, welke doelgroep is dan van toepassing en waarom?

- Zijn er aspecten van botnetbestrijding die ISP's toepassen die ontbreken in het referentiemodel?

- Welke aspecten die ISP's kunnen toepassen zijn op dit moment het meest effectief in de strijd tegen botnets? Welke aspecten waren in het verleden het meest effectief? Welke aspecten zijn waarschijnlijk voor de toekomst het meest effectief?

1.5 Niet ISP gerelateerde botnetbestrijdingsmethoden

In de literatuur worden voorstellen gedaan over hoe ISP's botnets kunnen bestrijden. Echter, niet alle voorstellen worden door ISP's toegepast. Hieronder is een lijst opgenomen met een aantal voorstellen die volgens de literatuur niet worden toegepast door ISP's.

Techniek	Omschrijving
Takedown	Het achterhalen en neerhalen van botnets.
Hack-back	Het overnemen van command and control servers om zo een botnet van binnenuit te bestrijden.
Infiltreren/manipuleren botnet	Het infiltreren in een botnet om de botnet zo van binnenuit te manipuleren.
Desinfecteren klant machine	Het op afstand ongevraagd desinfecteren van een klantmachine.
Opzeggen overeenkomst	Het opzeggen van een internetovereenkomst met een klant na meerdere botnetinfecties.
Blokkeren van website	Het actief blokkeren van websites waardoor klanten kunnen worden geïnfecteerd.

- In hoeverre klopt het dat bovenstaande voorstellen niet worden toegepast door ISP's?
- Ontbreken hierin nog zaken?

Bijlage 4: Lijst van security maatregelen voor ISP's

In Tabel 25 wordt een overzicht gegeven van maatregelen die ISP's kunnen gebruiken. Het uitleggen en verklaren van alle specifieke maatregelen valt buiten de scope van het afstudeeronderzoek.

Tabel 25 Overzicht maatregelen (Asghari, 2010)

Measure Category	Specific Measures
Active abuse handling	Provide contact details for email abuse and security violations
	Monitor RFC2412 addresses (abuse@domain, etc)
	React to complaints from other ISP's about security and spam (and track them)
	Respond to subscriber complaints about spam
	Abuse desk automation (using in-house system, ARF, and feedback loops)
	Keep public records of all publicly routable/visible IP addresses, and domain names (such as WHOIS, reverse DNS, SWIP, etc) correct, complete, and current.
Proactive detection of malicious activity	**Bot detection:**
	Monitor traffic peaks
	Monitor email bounces
	Actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and source of it
	Botnet detection via DNS
	Botnet detection via IP space scanning
	Botnet detection using NetFlow
	New threat detection:
	Deploy real-time traffic anomaly and/or signature based detection mechanism
	Use of blackholing and sinkholing to secure services
	Deploy spam-traps to optimize anti-spam installations
	Use in-house or 3rd party 'security intelligence service'
	Analyze where spam comes from
	Communicate and share data via feedback loops
Filtering malicious traffic and content	**Basic filtering (ingress and egress):**
	Block inbound port 25 (spam-relay)
	Block inbound port 53 to residential customers (avoid fast-flux)
	Manage access to outbound port 25 for hosts on residential network (spambots)
	Drop egress spoofed IP sources
	Content filtering (ingress and egress):
	HTTP: provide proxy service to filter bad web domains (phishing sites, etc)
	SMTP: anti-virus scan and spam-filters on network (e.g. during DATA phase)
	Block potentially infecting email attachments

	Inbound filtering of phishing messages
	Email content scanning: Bayesian filters, heuristic, probabilistic, frequency analysis, fingerprinting, URL-based, etc
	Disconnecting SMTP connections w/ unknown recipients
	Change incoming mail: disable hyperlinks, hide images from untrusted sources
	Outbound content filters (perform virus-scanning for outbound email,…)
	Dynamic filtering systems (based on IP reputation):
	Dynamic IP based sender reputation (also known as real-time-blacklists) - at IP level, or SMTP level
	Add offending subscribers to blacklist
	White-listing (ISP mail-servers, good customers)
	Short-lived blocks of web-traffic for suspicious sites
	Slowing suspicious traffic:
	Use of traffic shaping as a security method
	Grey-listing
	Slowing down SMTP connection
	Limit the volume of outbound mail
	Set greet pause in MTA
	Note: 'Ingress' traffic is applied to traffic coming from outside, where as 'egress' filtering is applied to traffic leaving the network.
User education and awareness	**Education, training, and campaigns:**
	Provide information on security via website or email (and other channels)
	Inform subscribers of risks of not implementing counter measures
	Provide educational literature to users with best practices for avoiding malware
	Use of customer portal for information
	Communicate security policies and procedures to subscribers
	Provide to users links for educational resources regarding nature and scope of threats
	Help in remediation:
	Notify users via email/telephone/walled-garden/in-browser/IM/SMS/ of infection
	Maintain a well-publicized security portal where a compromised user can be directed for remediation
	Provide security tools, education and useful links for users to perform own remediation
	Inform subscribers of costs of remedies and also point to professional help
	Detailed guidance to subscribers (provide a guided flow for remediation process)
	Maintain forum for users (self-help)

	Customer Call Support:
	Train call centre agents on how to assist users
	Abuse department customer dialog to help in disinfections
Client security and quarantining	**Disconnecting and quarantining infections:**
	Place infected users walled gardens (based on abuse report, or internal detection)
	Quarantine computer in networks unless protected
	Allow escape from walled garden if trusted, or if certain software is installed
	Service suspension on repeated security failures
	Service termination for non-compliant subscribers
	Walled garden measures – access lists; redirect HTTP; redirect botnet C&C to honeypot; manage outbound SMTP to quarantine/honeypot;
	Securing end user Clients:
	Provide security software (spam-filtering, anti-virus, browser plugins, etc) for clients, and encouraging their use. This can be for free or for a reasonable price
	Provide subscribers information about availability and use of such solutions with links
	Provide NAT routers with firewalls to customers
	Subject users to mandatory scan (when first provisioned, or periodic)
Using updated network protocols and servers	**Simple Mail Transfer Protocol:**
	SMTP Authentication: SMTP AUTH, TLS, Pop3 before SMTP,…
	Provide message submission for mail and ensure only account holders use it
	Use FQDN in EHLO/HELO
	Use sender validation (DKIM/Sender-id/SPF/reverseMX) on inbound email
	Reject email if detected forgery w/ sender authentication
	Prohibit sending of email with forged headers
	Configure human readable delivery status notifications (?)
	Other:
	Implement DNSSEC
	Ensure DNS architecture is up-to-date (to avoid cache poisoning)
Participation in the security community	**Membership:**
	Become member of an industry association
	Join one or more anti abuse forums
	Compare effectiveness of anti-spam installations with others?
	Share information and data on the intensity and scope of spam and its evolution
	Methods for sharing dynamic IP address space information with others
	Notification:

	Communicate knowledge of phishing attacks to the targeted institution
	Contact an ISP directly when receiving spam from it
	(allow spam source time to solve the problem before blocking traffic)
	Share evidence of bot with remote sites
	Implement / use feedback loops (e.g., between ETIS partners)
Management and administrative procedures	**Ensuring security level by adhering to:**
	Industry best practices
	National legislation guidance
	International standards (ISO 27002:2005, ISO 27006:2007)
	Using SLAs to ensure appropriate level of security
	Formal panning:
	Business contingency plan for protection of network integrity
	Disaster recovery plan for protection of network integrity
	Annual testing of business continuity plans
	Use a risk management process
	Other:
	Constantly improve knowledge and operating practices
	Review anti-spam installations for common practices?
	Multilevel abuse handling ?
	Build necessary tools for care agents to retrieve relevant info (about bot detection)
	Protect customer email addresses?
	Written security guidance for staff and subscribers
	Train support representatives about fishing and scams
Legal measures	Adopt and enforce Acceptable Use Policy (AUPs)
	Forbidding spamming in Terms and Conditions
	Informing subscribers of legal consequences of sending spam
	Inform NRA of security breach
	Inform customers / public of security breach
	Report spam to NRA (national authorities)
	Pursue legal actions for spam

Bijlage 5: Interviewverslagen

Uitwerking interviewverslag ISP1

Datum	**-**
Plaats	-

1 Algemene vragen

1.1 Geïnterviewde

Wat is uw naam (incl. voorletters, evt. titels)?
-
Wat is uw functie/relatie tot botnetbestrijding?
-
Wat zijn uw belangrijkste taken, verantwoordelijkheden en bevoegdheden?
-
Voor welke Internet Service Provider werkt u?
-

1.2 Organisatie

Wat is de naam van de organisatie waarvoor u werkt?
-
Hoe is op hoofdlijnen de organisatie ingericht? Maakt de organisatie deel uit van een grotere organisatie?
-
Zijn er openbare publicaties beschikbaar, zoals rapporten en jaarverslagen, van en over uw organisatie waarin cyber security in het algemeen of botnetbestrijding aan bod komt?
Jaarverslagen van de organisatie.

2. Samenwerkingsverbanden

Bent u bekend met samenwerkingsverbanden op het gebied van botnetbestrijding?
Ja
Welke samenwerkingsverbanden inzake botnetbestrijding kent u?
Forum for Incident Response and Security Teams (First). The IT Association for Telecommunications (ETIS). Binnen Nederland verschillende overlegorganen mede opgezet door de overheid (Nationaal Cyber Security Centrum).
Aan welke samenwerkingsverbanden neemt uw organisatie deel? Zo ja, is dit een samenwerkingsverband binnen Nederland, Europa of wereldwijd.
Door de ISP wordt er deelgenomen aan verschillende samenwerkingsverbanden: Forum for Incident Response and Security Teams (First)

The IT Association for Telecommunications (ETIS) Binnen Nederland actief in verschillende overlegorganen mede opgezet door de overheid (Nationaal Cyber Security Centrum) Op dit moment zijn er zoveel verschillende samenwerkingsverbanden actief dat er door ISP bewust keuzes worden gemaakt waaraan wordt deelgenomen.

3. **Botnets**

Welke definitie wordt binnen uw organisatie gehanteerd voor botnets?
Een netwerk van computers/apparaten die van afstand bestuurd worden vanaf een centraal punt (Centraal punt is tegenwoordig ook P2P) en die kunnen worden ingezet voor cybercriminaliteit.
Hoe worden botnets geclassificeerd?
Door de ISP worden botnets geclassificeerd. De classificatie richt zich vooral op wie er gevaar loopt, bijvoorbeeld de klant, de ISP en het netwerk.

4. Referentiemodel

Doelgroep	Aspect	Is dit aspect van toepassing voor uw organisatie?	Is de classificatie van het aspect juist? Zo nee, waarom niet en welke classificatie(s) is of zijn volgens u van toepassing op het aspect?	Is het aspect onderverdeeld in het juiste deelgebied? Zo nee, welk deelgebied is dan van toepassing en waarom?	Is het aspect toegekend aan de juiste doelgroep? Zo nee, welke doelgroep is dan van toepassing en waarom?	Opmerkingen	Technisch	Organisatorisch	Juridisch
Preventie									
Klant	P-1	Ja	Ja	Gedeeltelijk preventie, maar raakt ook verwijdering.	Ja	Heeft ook een commercieel aspect. Is niet gratis voor de klant. Is in abonnementsvorm voor een bepaald bedrag beschikbaar.	X	X	
	P-2	Ja	Nee, educatie van klanten is een organisatorische en juridische maatregel.	Ja, is onderverdeeld in het juiste deelgebied.	Ja	Door de ISP wordt uitleg gegeven. Dit heet veilig internetten. Veilig internetten is in één klik te vinden op de site van de ISP. Er zijn ook campagnes geweest vanuit de overheid. Het is een gedeelde verantwoordelijkheid tussen overheid en ISP. Er is een afspraak gemaakt met de overheid dat er een hyperlink is naar veilig internetten op de hoofdpagina van de provider.		X	X

Andere partijen	P-3	Ja	Ja	Ja	Ja	Publiek wordt het niet gedeeld. Klanten worden geïnformeerd dat de ISP er iets mee doet via de Abuse website van de provider. Door de ISP wordt actief gecommuniceerd binnen de gemeenschap over procedures. De overheid speelt hier een centrale rol in.		X	
	P-4	Ja	Ja, maar is ook technisch van aard.	Ja, is onderverdeeld in het juiste deelgebied. Raakt ook detectie notificatie en herstel.	Ja	De ISP is actief binnen verschillende samenwerkingsverbanden. Door de ISP wordt er actief deelgenomen in samenwerkingsverbanden op nationaal, Europees en wereldwijd gebied.	X	X	
ISP intern	P-5	Nee				De ISP maakt geen gebruik van een IPS.			
	P-6	Nee				Er worden geen technische maatregelen genomen tegen botnets. Dit mag ook niet zo snel meer vanwege de netneutraliteit.			
	P-7	Beperkt	Ja	Nee, valt onder detectie.	Nee, dit gebeurt in een samenwerkingsverband. Dit is te complex om nog alleen op te pakken.	Rol van het CERT team binnen de ISP.	X	X	
	P-8	Ja	Ja	Nee, valt onder detectie, notificatie, verwijdering en herstel	Ja	Binnen de organisatie zijn de processen gedocumenteerd.		X	

	P-9	Ja	Ja	Nee, valt onder notificatie, verwijdering en herstel. (niet detectie gedeelte)	Ja	Binnen de ISP is een abuseteam actief. Het abuseteam komt pas in actie bij notificatie, verwijdering en herstel.	X	X	
	P-10	Ja	Ja	Ja	Ja	Door de ISP zijn er SLA's ingericht met betrekking tot botnetbestrijding.		X	
	P-11	Ja	Ja	Ja	Ja	Door de ISP wordt er gebruik gemaakt van standaardisering met betrekking tot botnetbestrijding. Door de ISP wordt aangegeven dat het ook juridisch van aard is, omdat er gewerkt wordt met klantgegevens.		X	
Detectie									
Klant	D-1	Beperkt	Nee, is technisch van aard. Het is een tool waarmee de klant kan checken of recente updates zijn geïnstalleerd.	Nee, valt onder preventie.	Ja	Ja, er is een beperkte veiligheidsscan die klanten kunnen uitvoeren via de website van de ISP. Het bevindt zich op het niveau van besturingssysteem en applicaties. De check controleert of de klant de meest recente updates heeft geïnstalleerd met betrekking tot besturingssysteem en applicaties.	X		
	D-2	Ja	Ja	Nee, valt onder verwijdering en herstel.	Ja	De ISP krijgt feedback van klanten. Het is een belangrijk onderdeel van het abuse proces.		X	

Andere partijen	D-3	Nee				Door de ISP worden gedetecteerde besmettingen niet gedeeld met andere ISP's. Meestal ontvangt de ISP informatie van andere partijen met betrekking tot besmettingen.			
	D-4	Ja	Ja	Ja	Ja	100 % van de input, omdat de ISP zelf niet mag detecteren.		X	
	D-5	Ja	Ja	Ja	Ja	De ISP is lid van de vereniging Abuse Information Exchange en ontvangt informatie over mogelijke besmettingen van de AbuseHub.		X	
ISP intern	D-6	Nee				De ISP zelf gebruikt geen honeypots om besmettingen in zijn eigen netwerk te detecteren. In het netwerk van de ISP staan wel honeypots, maar die zijn onderdeel van het honeynetproject.			
	D-7	Ja	Ja	Valt onder notificatie.	Nee, raakt andere partijen. Notificatie vanuit extern en informatie naar de klant.	Doordat de ISP zelf geen besmettingen detecteert, maar daarop wordt gewezen door andere partijen, valt deze niet onder detectie maar onder notificatie. De actie hierop kan zijn het notificeren van de klant.		X	
	D-8	Nee				Wordt alleen gebruikt voor de eigen infrastructuur.			

Notificatie									
Klant	N-1	Ja	Ja	Ja	Ja	Door de ISP wordt melding gedaan aan de geïnfecteerde klant. Het aspect is onderverdeeld in het juiste deelgebied.		X	
	N-2	Ja	Ja	Ja	Nee, is specifiek voor de klant. Er wordt door de ISP verwezen naar externe partijen.	Door de ISP wordt aangegeven dat dit cruciaal is. Stel dat een ISP een probleem meldt dan is de eerste vraag van de klant hoe los ik dit op. Door de ISP wordt de eerste melding daarom zo zorgvuldig mogelijk gedaan. Uitleg over het probleem, de oorzaak en hoe het probleem kan worden opgelost. Daarnaast nog tips en trucs om de gebruiker te helpen. De ISP probeert hierin ook een stukje preventie mee te nemen om herhaling te voorkomen.	X	X	
Andere partijen	N-3	Nee				Door de ISP wordt geen melding gedaan aan andere partijen.			
	N-4	Ja				Wordt geen meldingen gedaan bij de ACM inzake botnets. Er is geen verplichting om dit te doen.			
Verwijdering/bestrijding									
Klant	V-1	Ja	Ja	Ja, valt ook onder notificatie. Door de ISP	Ja	Door de ISP worden geïnfecteerde gebruikers geïsoleerd.	X	X	

				wordt de walled garden ook voor notificatie ingezet.					
	V-2	Ja	Ja	Ja	Ja	Door de ISP wordt informatie gedeeld omtrent het oplossen van botnetinfecties.	X		
	V-3	Ja	Ja	Ja	Ja	De ISP heeft links naar professionele hulp.	X		
Klant / Andere partijen	V-4	Ja	Ja	Ja	De ISP deelt de procedure van de werking van de walled garden met de klant. Binnen de gemeenschap worden de best pratices en technieken gedeeld. Dit aspect kan worden opgedeeld in klant en andere partijen.	De ISP deelt de best practices met de gemeenschap. Via de website wordt informatie gedeeld over hoe de walled garden wordt ingezet.	X	X	
Andere partijen	V-5	Ja	Ja	Ja, valt ook onder notificatie. Door de ISP worden ook best practices gedeeld over notificatie.	Binnen de vereniging Abuse Information Exchange zijn er bijeenkomsten waar de best practices worden gedeeld. Best practices worden gedeeld met andere partijen.	Door de ISP worden best practices gedeeld inzake gebruik van de walled garden.	X	X	
Herstel									
Klant	H-1	Ja	Ja	Ja	Ja	De klant maakt zelf ook onderdeel uit van dit proces. De klant kan zelf in veel gevallen besluiten wanneer hij zijn verbinding weer activeert.		X	
	H-2	Nee				Door de ISP worden klanten niet ondersteunt in herstel.			

	H-3	Ja	Ja	Ja	Ja	Klanten worden geïnformeerd over de gevolgen van een infectie. De ISP streeft er naar dat het verwijderen/herstellen geen impact heeft.	X	X	
	H-4	Nee				Door de ISP wordt geen informatie beschikbaar gesteld over het herstellen van de data. Verantwoordelijkheid van de klant zelf.			

Zijn er aspecten van botnetbestrijding die ISP's toepassen die ontbreken in het referentiemodel?
Nee
Welke aspecten zijn het meest effectief in de strijd tegen botnets op dit moment?
Preventie en notificatie.
Welke aspecten waren in het verleden effectief in de strijd tegen botnets?
Preventie.
Welke aspecten zijn volgens u effectief in de toekomst?
Preventie blijft het meest cruciaal. Banners/websites veiliger maken.

5. Niet ISP gerelateerde botnetbestrijdingsmethoden

In hoeverre klopt het dat bovenstaande voorstellen niet worden toegepast door ISP's?
De ISP is wel betrokken bij notice en takedown. Het kan in theorie zo zijn dat er een C&C server bij een klant staat. Dan kan er een melding binnen komen met het verzoek tot takedown. Binnen de ISP is er een proces beschreven voor notice and takedown. De takedown zal dan snel plaatsvinden. De ISP kan zelf ook een notice en takedown verzoek opstarten.
Ontbreken hierin nog zaken?
Nee

6. Opmerkingen

Extra
Door de ISP wordt er gebruik gemaakt van een abuse emailadres waar meldingen met betrekking tot abuse en security kunnen binnen komen. Komt er een melding binnen, dan wordt het proces gestart. Door de ISP wordt duidelijk aangegeven dat er geen gebruik wordt gemaakt van detectiesystemen binnen het netwerk om klantverkeer te monitoren. Er wordt dus geen IPS en IDS ingezet in de bestrijding van botnets op het netwerk van de ISP. Op de website van de ISP is op de hoofdpagina een verwijzing naar veilig internetten om klanten te informeren over de risico van het internet.
Neemt de ISP maatregelen tegen degenen die het botnet beheren/aansturen, dus tegen de infectoren?
Door de ISP wordt aangegeven dat er alleen acties worden ondernomen tegen bots. Het ondernemen van acties tegen botnetstructuren en botmasters is een taak die is weggelegd voor de overheid.

Uitwerking interviewverslag ISP2

Datum	10 juni 2015
Plaats	-

1 Algemene vragen

1.1 Geïnterviewde

Wat is uw naam (incl. voorletters, evt. titels)?

-

Wat is uw functie/relatie tot botnetbestrijding?

-

Wat zijn uw belangrijkste taken, verantwoordelijkheden en bevoegdheden?

-

Voor welke Internet Service Provider werkt u?

-

1.2 Organisatie

Wat is de naam van de organisatie waarvoor u werkt?

-

Hoe is op hoofdlijnen de organisatie ingericht? Maakt de organisatie deel uit van een grotere organisatie?

-

Zijn er openbare publicaties beschikbaar, zoals rapporten en jaarverslagen, van en over uw organisatie waarin cyber security in het algemeen of botnetbestrijding aan bod komt?

-

2. Samenwerkingsverbanden

Bent u bekend met samenwerkingsverbanden op het gebied van botnetbestrijding?

Ja, de ISP neemt deel aan verschillende samenwerkingsverbanden.

Welke samenwerkingsverbanden inzake botnetbestrijding kent u?

- AbuseHUB
- o-IRT-o
- ECP
- Botfrei.de
- AC/DC

Aan welke samenwerkingsverbanden neemt uw organisatie deel? Zo ja, is dit een samenwerkingsverband binnen Nederland, Europa of wereldwijd.

De ISP neemt actief deel aan de AbuseHUB en de o-IRT-o. De ISP is alleen actief in samenwerkingsverbanden binnen Nederland.

3. Botnets

Welke definitie wordt binnen uw organisatie gehanteerd voor botnets?
Een botnet is een netwerk van systemen die ongewenst op afstand beheerd/bestuurd worden.
Hoe worden botnets geclassificeerd?
Door de ISP worden botnets niet geclassificeerd. Als de ISP een botnet bestrijdt, is dit altijd in samenwerking met NCSC. NCSC heeft dan de botnet geclassificeerd. De ISP classificeert wel abuse, maar geen botnets.

4. Referentiemodel

Preventie									
Doelgroep	Aspect	Is dit aspect van toepassing voor uw organisatie?	Is de classificatie van het aspect juist? Zo nee, waarom niet en welke classificatie(s) is of zijn volgens u van toepassing op het aspect?	Is het aspect onderverdeeld in het juiste deelgebied? Zo nee, welk deelgebied is dan van toepassing en waarom?	Is het aspect toegekend aan de juiste doelgroep? Zo nee, welke doelgroep is dan van toepassing en waarom?	Opmerkingen	Technisch	Organisatorisch	Juridisch
Klant	P-1	Ja	Ja	Bescherming en preventie.	Ja	Virusscanner en een walled garden ter bescherming van de klant. Geen diensten waar de nadruk op security ligt. De klant moet worden beschermd, maar het internet ook tegen de klant. De ISP heeft een zorgplicht. Als er bijvoorbeeld een security probleem is met een router is de ISP verplicht de klant te informeren en maatregelen te nemen.	X	X	
	P-2	Ja	Ja	Ja	Ja	Zelfstandig en in combinatie met ECP. Bijvoorbeeld de digibewust campagne. De ISP verstuurt met regelmaat nieuwsbrieven aan hun klanten met informatie over bijvoorbeeld botnets, ransomware.		X	
Andere partijen	P-3	Ja	Ja	Ja	Ja	De ISP deelt informatie binnen de samenwerkingsverbanden, bijvoorbeeld in de AbuseHUB en in de o-IRT-o.		X	
	P-4	Ja	Ja	Ja	Ja	De ISP neemt deel aan samenwerkingsverbanden.		X	

ISP intern	P-5	Nee				De ISP maakt geen gebruik van een IPS met betrekking tot het klantverkeer. De ISP is van mening dat de walled garden in feite ook een IPS is, maar deze wordt niet gevoed door verkeer te filteren. Het maakt gebruik van externe bronnen. Het systeem wordt gevoed door bijvoorbeeld mailservers, informatie van de shadow server organisatie en nog een aantal externe bronnen.			
	P-6	Beperkt	Ja	Nee, is ter bestrijding	Ja	Als er meldingen komen inzake botnetbesmettingen, vanuit bijvoorbeeld de o-IRT-o, kan er besloten worden technische matregelen te nemen. Dit kunnen maatregelen zijn zoals extra firewallregels of een klant in de walled garden omgeving plaatsen.	X		
	P-7	Ja	Ja	Ja	Nee, wordt samen gedaan met andere partijen. Dit in verband met schaalgrootte.	Wordt gedaan door het Security Operations Center (SOC) dat actief is bij de ISP.	X	X	
	P-8	Ja	Ja	Nee, beslaat meerdere gebieden. Verwijdering/bestrijding	Ja	Er is binnen de ISP een abuse afdeling actief. Het team wordt ingezet voor verwijdering en bestrijding.		X	
	P-9	Ja		Voor verwijdering en bestrijding		Binnen de ISP is een abuse afdeling actief.		X	
	P-10	Nee				Geen SLA met betrekking tot botnetbestrijding.			

	P-11	Wens	Ja	Ja	Ja	Nog niet, is een wens. Er is een Security Operations Center (SOC) opgericht. ISO certificering is een doel voor de toekomst.		X	
Detectie									
Klant	D-1	Beperkt	Ja	Ja	Ja	Er wordt verwezen vanuit de walled garden naar externe publieke portals. Het is de bedoeling om in de toekomst remediation tools te gaan aanbieden.	X		
	D-2	Nee				Door de ISP wordt geen informatie van klanten ontvangen met betrekking tot botnetbesmettingen.			
Andere partijen	D-3	Ja	Ja	Ja	Ja	De ISP communiceert besmettingen naar andere partijen.	X	X	
	D-4	Ja	Ja	Ja	Ja	De ISP ontvangt informatie over mogelijke besmettingen via de AbuseHUB.		X	
	D-5	Ja	Ja	Ja	Ja	Vanuit de AbuseHUB worden de meldingen over besmettingen doorgegeven aan de ISP.		X	
ISP intern	D-6	Ja	Ja	Ja	Ja	Staan binnen het netwerk van de ISP, maar zijn van een externe partij.	X		
	D-7	Ja	Ja	Ja	Ja	Geen SLA hiervoor dus geen reactietermijn gedefinieerd. Het is wel de bedoeling van de ISP om zo snel mogelijk te reageren.		X	
	D-8	Nee				De ISP heeft geen IDS. De ISP heeft niet de intentie om een IDS in te zetten voor klantverkeer.			
Notificatie									

Klant	N-1	Ja	Ja	Ja	Ja	De ISP informeert de klant via een walled garden of email en heel af toe via de telefoon		X	
	N-2	Ja	Ja	Ja	Ja	Op het moment dat een klant is geïnfecteerd, kan de klant worden doorverwezen via de walled garden naar een tool die het probleem kan oplossen. De klant krijgt via de walled garden links naar een mogelijke oplossing.	X	X	
Andere partijen	N-3	Ja	Ja	Ja	Ja	Via bijvoorbeeld o-IRT-o		X	
	N-4	Nee				Indien er klantgegevens worden gelekt door de ISP moet dit worden gemeld bij de ACM. Ook moet de klant worden geïnformeerd over het probleem. Indien een klant een botnetbesmetting heeft, wordt dit door de ISP niet gemeld bij de ACM. Wel heeft de ISP na de klant een zorgplicht als de klant geïnfecteerd is met een botnet.			
Verwijdering/bestrijding									
Klant	V-1	Ja	Ja	Preventie naar andere klanten. Klanten moeten gewaarschuwd worden voor de risico's.	Ja	De ISP isoleert gebruikers via de walled garden. De ISP doet dit ook vanuit preventie om mensen te wijzen gevaren.	X	X	
	V-2	Ja	Ja	Ja	Ja	De ISP verwijst vanuit de walled garden naar een mogelijke oplossing. Ook kan er verwezen worden naar professionele hulp.	X	X	

	V-3	Beperkt	Ja	Ja	Ja	Door de ISP wordt er verwezen naar professionele hulp.		X	
Klant / Andere partijen	V-4	Ja	Ja	Ja	Ja	Door de ISP wordt aan de klant uitgelegd hoe om te gaan met de walled garden. De technische procedure wordt niet gedeeld met de klant. Binnen de verschillende samenwerkingsverbanden is wel gedeeld hoe de walled is functioneert en hoe het technisch is opgebouwd. Beter is om dit aspect onder te verdelen in twee delen (klant en andere partijen).		X	
Andere partijen	V-5	Nee				Door de ISP worden geen best practices gedeeld met andere partijen.			
Herstel									
Klant	H-1	Ja	Ja	Ja	Ja	Door de ISP wordt bepaald wanneer de klant uit de walled garden omgeving gaat.	X	X	
	H-2	Ja	Ja	Ja	Ja	Er is binnen de ISP een abuse afdeling actief. Als klanten naar de abuse afdeling bellen, worden ze geholpen. Er is wel een beperking aan de mate van hulp.	X	X	
	H-3	Ja	Ja	Ja	Ja	Als het risico groot is, wordt de klant hierop gewezen.		X	
	H-4	Beperkt	Ja	Ja	Ja	Er wordt beperkt informatie beschikbaar gesteld met betrekking tot herstel.	X		

Zijn er aspecten van botnetbestrijding die ISP's toepassen die ontbreken in het referentiemodel?
Het opgestelde referentiemodel dekt de lading
Welke aspecten zijn het meest effectief in de strijd tegen botnets op dit moment?
Snelheid van handelen is het meest effectief. Daarnaast is het in quarantaine plaatsen van machines effectief en het delen van abuse informatie. Door de ISP wordt aangegeven dat sinds de NCSC zijn rol heeft opgepakt in de strijd tegen botnets dit een positief effect heeft gehad op de bestrijding van botnets.
Welke aspecten waren in het verleden effectief in de strijd tegen botnets?
-
Welke aspecten zijn volgens u effectief in de toekomst?
Door de ISP wordt aangegeven dat ze hopen de strijd tegen botnets te winnen, maar dit een lastig gevecht is.

5. Niet ISP gerelateerde botnetbestrijdingsmethoden

In hoeverre klopt het dat bovenstaande voorstellen niet worden toegepast door ISP's?
De ISP is het eens met de lijst. In extreme gevallen kan het voorkomen dat een website wordt geblokkeerd. De ISP krijgt takedown verzoeken maar niet met betrekking tot botnets.
Ontbreken hierin nog zaken?
Volgens de ISP ontbreekt in de lijst nog het beïnvloeden van het klantverkeer. Dit wordt door de ISP niet gedaan.

Extra

Neemt de ISP maatregelen tegen degenen die het botnet beheren/aansturen, dus tegen de infectoren?
De ISP is van mening dat zij hiervoor te klein zijn.

Uitwerking interviewverslag ISP3

Datum	**-**
Plaats	30-6-2015

1 Algemene vragen

1.1 Geïnterviewde

Wat is uw naam (incl. voorletters, evt. titels)?
-
Wat is uw functie/relatie tot botnetbestrijding?
-
Wat zijn uw belangrijkste taken, verantwoordelijkheden en bevoegdheden?
-
Voor welke Internet Service Provider werkt u?
-

1.2 Organisatie

Wat is de naam van de organisatie waarvoor u werkt?
-
Hoe is op hoofdlijnen de organisatie ingericht? Maakt de organisatie deel uit van een grotere organisatie?
-
Zijn er openbare publicaties beschikbaar, zoals rapporten en jaarverslagen, van en over uw organisatie waarin cyber security in het algemeen of botnetbestrijding aan bod komt?
Door de organisatie worden er verschillende documenten gepubliceerd met betrekking tot cyber security. Bijvoorbeeld jaarverslagen, dreigingsbeeld, expert opinion en innovatiebrochure 2014.

2. Samenwerkingsverbanden

Bent u bekend met samenwerkingsverbanden op het gebied van botnetbestrijding?
Ja
Welke samenwerkingsverbanden inzake botnetbestrijding kent u?
The honeynet project / honeyned chapter Nederland o-IRT-o Vereniging Abuse information Exchange First Squid AC/DC
Aan welke samenwerkingsverbanden neemt uw organisatie deel? Zo ja, is dit een samenwerkingsverband binnen Nederland, Europa of wereldwijd.
The honeynet project / honeyned chapter Nederland o-IRT-o Vereniging Abuse information Exchange First Squid

Extra

De ISP levert internet aan instellingen die deze zelf weer doorgeven aan hun klanten. De geïnterviewde ISP heeft instellingen als klant.

3. Botnets

Welke definitie wordt binnen uw organisatie gehanteerd voor botnets?
Door de ISP wordt er geen definitie gehanteerd. Er wordt gekeken of iets mogelijk besmet is en hier wordt melding van gemaakt.
Hoe worden botnets geclassificeerd?
Door de ISP wordt er geclassificeerd op de volgende wijze: geïnfecteerd of niet geïnfecteerd.

4. Referentiemodel

Preventie									
Doelgroep	Aspect	Is dit aspect van toepassing voor uw organisatie?	Is de classificatie van het aspect juist? Zo nee, waarom niet en welke classificatie(s) is of zijn volgens u van toepassing op het aspect?	Is het aspect onderverdeeld in het juiste deelgebied? Zo nee, welk deelgebied is dan van toepassing en waarom?	Is het aspect toegekend aan de juiste doelgroep? Zo nee, welke doelgroep is dan van toepassing en waarom?	Opmerkingen	Technisch	Organisatorisch	Juridisch
Klant	P-1	Beperkt	Ja	Ja	Ja	De ISP stelt geen endpoint security oplossingen beschikbaar voor haar klanten. De ISP gaat er van uit dat de klanten hierin zelf actie ondernemen. Door de ISP worden af en toe endpoint security producten getest op werking. Daarnaast helpt de ISP haar klanten met bijvoorbeeld toegangsregels voor de firewall.	X		
	P-2	Ja	Ja	Ja	Ja	De ISP neemt hierin actief deel door bijeenkomsten te organiseren/faciliteren voor haar klanten. De ISP probeert de security awareness van de klanten te verhogen. De ISP traint ook het CERT van de bij hun aangesloten klanten.	X	X	X
	P-3	Ja	Ja	Valt ook gedeeltelijk onder detectie.	Nee, heeft ook betrekking op klanten.	Door de ISP wordt actief informatie gedeeld binnen de verschillende samenwerkingsverbanden, zoals de vereniging Abuse Information Exchange en o-IRT-o.	X	X	

Andere partijen	P-4	Ja	Ja	Ja	Ja	Door de ISP wordt actief deelgenomen in verschillende samenwerkingsverbanden. Het is een doelstelling van de ISP om middelen ter beschikking te stellen aan onderzoeksinstellingen die trachten botnets te bestrijden. De ISP zoekt grenzen op wat wel en niet mag inzake botnetbestrijding. De ISP publiceert hier tevens over.	X	X	X
ISP intern	P-5	Nee				Door de ISP wordt geen IPS ingezet.			
	P-6	Nee				De ISP is van mening dat dit de verantwoordelijkheid van de klant zelf is.			
	P-7	Ja	Ja	Ja	Ja	Door de ISP wordt actief de laatste stand van zaken gevolgd met betrekking tot botnet/malware technieken. Dit wordt gedaan door het bijwonen van conferenties. Daarnaast zijn de medewerkers van het CERT van de ISP actief in het onderhouden van contacten met andere specialisten op het gebied van botnet/malware technieken.	X	X	
	P-8	Ja	Ja	Ja	Ja	Door de ISP zijn er processen ingericht met betrekking tot incident response. Zodra er een incident is, wordt dit actief en gestructureerd opgepakt. Hiervoor zijn verschillende processen ingericht.	X	X	
	P-9	Ja	Ja	Ja, is ook onderdeel van detectie	Ja	Binnen de ISP bestaat een actieve Computer emergency response	X	X	

						team. Het CERT van de ISP is 24x7 actief.			
	P-10	Ja	Ja	Ja	Ja	De ISP maakt gebruik van Service Level Specifications (SLS).		X	
	P-11	Beperkt	Ja	Ja	Ja	Door de ISP wordt er geen gebruik gemaakt van ISO certificering. De ISP voert intern wel audits uit, bijvoorbeeld een maturity scan. Er bestaat wel de wens om in de toekomst te gaan certificeren.	X	X	
Detectie									
Klant	D-1	Nee				Door de ISP wordt geen portal aangeboden waarop klanten kunnen testen op infecties.			
	D-2	Beperkt	Ja	Ja	Ja	De ISP geeft aan dat dit incidenteel kan voorkomen.	X		
Andere partijen	D-3	Ja	Ja	Ja	Ja	De ISP geeft aan dat dit de één van de belangrijkste taken is. De meldingen die binnen komen, worden doorgegeven aan de aangesloten klanten.	X	X	
	D-4	Ja	Ja	Ja	Ja	Door de ISP wordt er van verschillende externe bronnen informatie ontvangen over mogelijke besmettingen binnen hun netwerk. Eén van deze externe bronnen is Shadowserver. Door de ISP wordt deze informatie doorgezet naar de bij hun aangesloten klanten die hierop actie kunnen ondernemen.	X	X	

	D-5	Ja	Ja	Ja	Ja	De ISP ontvangt informatie vanuit de AbuseHUB. De informatie kan vanwege technische redenen nog niet worden gedeeld met klanten. Door de ISP wordt aangegeven dat dit wordt opgepakt.	X	X	
ISP intern	D-6	Nee				De ISP maakt zelf geen gebruik van honeypots. De ISP faciliteert echter wel verschillende onderzoeksinstellingen. Dit kan betekenen dat er ook honeypots/sinkholes worden gehost op de beschikbaar gestelde faciliteiten.			
	D-7	Ja	Ja	Ja	Ja	Door het CERT team van de ISP wordt er op zo kort mogelijke termijn gereageerd op incidenten (binnen een dag). Vervolgens is het zaak dat de bij hun aangesloten klanten het oppikken en er mee aan de slag gaan.	X	X	
	D-8	Beperkt	Ja	Ja	Ja	Als er door de ISP bijvoorbeeld hoge packet rates worden gedetecteerd in hun netwerk kunnen er extra middelen worden ingezet om het probleem te analyseren. De ISP geeft aan geen gebruik te maken van een IDS. Echter, heeft de ISP wel een analysedienst die verkeersgegevens van de klanten kan analyseren om netwerkaanvallen te kunnen detecteren (Netflow)	X		
Notificatie									

Klant	N-1	Ja	Ja	Ja	Ja	Door de ISP worden klanten via email geïnformeerd over mogelijke besmettingen. Indien de klant hierop geen actie onderneemt, kan er ook telefonisch contact worden gelegd. In noodgevallen kan de ISP besluiten om de verbinding van de klant te verbreken.	X	X	
Andere partijen	N-2	Beperkt	Ja	Ja	Ja	Het kan voorkomen dat de ISP, op het moment dat hij een klant informeert over een mogelijke besmetting, informatie meestuurt over hoe dit op te lossen.	X	X	
	N-3	Ja	Ja	Ja	Ja	De ISP krijgt informatie vanuit de bij hun actieve sinkholes. Deze informatie wordt eerst met hun eigen klanten gedeeld alvorens dit met andere partijen wordt gedeeld.	X	X	
	N-4	Nee				Doordat de ISP geen diensten aanbiedt aan eindgebruikers heeft de ISP een uitzonderlijke positie.			
Verwijdering/bestrijding									
Klant	V-1	Nee				Het is mogelijk dat de klanten van de ISP zelf systemen actief hebben om gebruikers in zogenaamde walled gardens te plaatsen.			
	V-2	Ja	Ja	Ja	Ja	Het is mogelijk dat de ISP informatie deelt met de klanten over een mogelijke oplossing voor een besmetting.	X	X	
	V-3	Nee				Door de ISP wordt aangegeven dat de klant zelf goed in staat is om professionele hulp in te schakelen.			

Klant / Andere partijen	V-4	Nee				De ISP heeft geen walled garden actief.			
Andere partijen	V-5	Ja	Ja	Ja	Ja	Door de ISP wordt aangegeven dat, als het succesvol heeft meegewerkt aan het bestrijden van een botnet en het is publicatiewaardig, ze hierover publiceren.	X	X	
Herstel									
Klant	H-1	Nee				Dit aspect is niet van toepassing voor de ISP, omdat de ISP geen consumenten als klant heeft.			
	H-2	Nee				Dit aspect is niet van toepassing voor de ISP, omdat de ISP geen consumenten als klant heeft.			
	H-3	Nee				Dit aspect is niet van toepassing voor de ISP, omdat de ISP geen consumenten als klant heeft.			
	H-4	Nee				Dit aspect is niet van toepassing voor de ISP, omdat de ISP geen consumenten als klant heeft.			

Zijn er aspecten van botnetbestrijding die ISP's toepassen die ontbreken in het referentiemodel?
Door de ISP wordt aangegeven dat in het model geen aandacht wordt besteed aan geïnfecteerde websites die worden ingezet voor bijvoorbeeld een DDoS aanval. Op dit moment veroorzaken besmette websites veel problemen.
Welke aspecten zijn het meest effectief in de strijd tegen botnets op dit moment?
Het is van belang om snel te reageren.
Welke aspecten waren in het verleden effectief in de strijd tegen botnets?
Snelle detectie en snelle notificatie.
Welke aspecten zijn volgens u effectief in de toekomst?
Snelle detectie en snelle notificatie.

5. Niet ISP gerelateerde botnetbestrijdingsmethoden

In hoeverre klopt het dat bovenstaande voorstellen niet worden toegepast door ISP's?
De ISP geeft wel gehoor aan notice en takedown verzoeken. De ISP faciliteert bijvoorbeeld wel onderzoeksinstellingen die proberen een botnet neer te halen, te infiltreren of te manipuleren. Door de ISP wordt aangegeven dat de onderzoeksinstellingen hiermee af en toe grenzen opzoeken van wat juridische toelaatbaar is in de strijd met botnets.
Ontbreken hierin nog zaken?
-

Extra

Neemt de ISP maatregelen tegen degenen die het botnet beheren/aansturen, dus tegen de infectoren?
De ISP zelf neemt geen maatregelen tegen bots, botnet-structuur of botmasters. De ISP faciliteert wel onderzoeksinstellingen die proberen bijvoorbeeld een botnet te infiltreren.

Uitwerking interviewverslag ISP4

Datum	6-7-2015
Plaats	-

1 Algemene vragen

1.1 Geïnterviewde

Wat is uw naam (incl. voorletters, evt. titels)?
-
Wat is uw functie/relatie tot botnetbestrijding?
-
Wat zijn uw belangrijkste taken, verantwoordelijkheden en bevoegdheden?
-
Voor welke Internet Service Provider werkt u?
-

1.2 Organisatie

Wat is de naam van de organisatie waarvoor u werkt?
-
Hoe is op hoofdlijnen de organisatie ingericht? Maakt de organisatie deel uit van een grotere organisatie?
-
Zijn er openbare publicaties beschikbaar, zoals rapporten en jaarverslagen, van en over uw organisatie waarin cyber security in het algemeen of botnetbestrijding aan bod komt?
Door de ISP wordt aangegeven dat het af en toe bijdraagt aan een publicatie, bijvoorbeeld met betrekking tot ISO certificering.

2. Samenwerkingsverbanden

Bent u bekend met samenwerkingsverbanden op het gebied van botnetbestrijding?
Ja, de ISP is bekend met samenwerkingsverbanden.
Welke samenwerkingsverbanden inzake botnetbestrijding kent u?
Vereniging Abuse Information Exchange Daarnaast is de ISP bekend met andere samenwerkingsverbanden met betrekking tot security.
Aan welke samenwerkingsverbanden neemt uw organisatie deel? Zo ja, is dit een samenwerkingsverband binnen Nederland, Europa of wereldwijd.
De ISP is actief binnen de Vereniging Abuse Information Exchange. Door de ISP wordt aangegeven dat zij sinds het begin betrokken zijn bij de opzet van de Vereniging Abuse Information Exchange.

3. Botnets

Welke definitie wordt binnen uw organisatie gehanteerd voor botnets?
Botnets zijn computers die centraal worden aangestuurd en die samenwerken. Het doel hiervan is dat de besmette machines misbruikt worden voor bijvoorbeeld een DDoS aanval.
Hoe worden botnets geclassificeerd?
De ISP geeft aan dat botnets zelf niet specifiek worden geclassificeerd, maar besmettingen in het algemeen wel. De volgende kwalificaties worden gebruikt: - De klant is een gevaar voor anderen. - De klant heeft alleen zelf een probleem. - De klant is kwetsbaar en kan mogelijk geïnfecteerd raken waarna hij een gevaar voor anderen kan worden.

4. Referentiemodel

Preventie									
Doelgroep	Aspect	Is dit aspect van toepassing voor uw organisatie?	Is de classificatie van het aspect juist? Zo nee, waarom niet en welke classificatie(s) is of zijn volgens u van toepassing op het aspect?	Is het aspect onderverdeeld in het juiste deelgebied? Zo nee, welk deelgebied is dan van toepassing en waarom?	Is het aspect toegekend aan de juiste doelgroep? Zo nee, welke doelgroep is dan van toepassing en waarom?	Opmerkingen	Technisch	Organisatorisch	Juridisch
Klant	P-1	Ja	Ja	Ja	Ja	Door de ISP wordt er standaard een router geleverd met extra security features. Binnen de ISP bestaat ook de mogelijkheid tot het afnemen van een extra abonnement voor extra bescherming. Dit is echter tegen betaling.	X	X	
	P-2	Ja	Ja	Ja	Ja	Door de ISP wordt aangegeven dat hier aandacht voor is. Daarnaast publiceert de ISP een nieuwsbrief waarin aandacht is voor veiligheid. Dit aspect kan ook als juridisch worden aangemerkt, omdat de ISP van mening is dat hij een zorgplicht heeft naar zijn klanten.	X	X	X
Andere partijen	P-3	Ja	Ja	Ja, kan ook voor detectie zijn.	Ja	De ISP deelt met andere ISP's informatie omtrent botnetbestrijding.		X	
	P-4	Ja	Ja	Ja	Ja	Door de ISP wordt aangegeven dat er actief wordt deelgenomen in de vereniging Abuse Information Exchange.		X	

ISP intern	P-5	Nee				De ISP maakt geen gebruik van een IPS, maar heeft wel bijvoorbeeld een systeem actief om bijvoorbeeld spam te voorkomen.			
	P-6	Ja	Ja	Ja	Ja	De ISP geeft aan dat in sommige gevallen er technische maatregelen kunnen worden genomen inzake botnets. Dit hangt echter erg van de situatie af. Dit wordt per afzonderlijk geval beoordeeld.	X		
	P-7	Beperkt	Ja	Ja	Ja	Door de ISP wordt aangegeven dat er aandacht is voor het bijhouden van de stand van zaken met betrekking tot malware, maar niet specifiek voor botnets.	X	X	
	P-8	Ja	Ja	Ja	Ja	De ISP heeft processen ingericht omtrent klantondersteuning. De ISP heeft geen specifieke processen ingericht met betrekking tot botnetbestrijding. Dit is onderdeel van het malwareproces.		X	
	P-9	Ja	Ja	Ja	Ja	Binnen de ISP is er geen specifiek abuse afdeling. Echter, er zijn verschillende mensen met een abusedesk rol.		X	
	P-10					Er zijn geen SLA's ingericht met betrekking tot botnets.		X	
	P-11	Ja	Ja	Ja	Ja	De organisatie doet aan standaardisering inzake beveiliging.	X	X	X
Detectie									

Klant	D-1	Nee				Op dit moment heeft de ISP geen self-identify portal actief.			
	D-2	Nee				De ISP ontvangt geen informatie omtrent besmettingen van hun klanten			
Andere partijen	D-3	Beperkt	Ja	Ja	Ja	Door de ISP wordt aangegeven dat dit op beperkte schaal plaatsvindt.		X	
	D-4	Ja	Ja	J	Ja	De ISP ontvangt informatie met betrekking tot botnetbesmettingen van de AbuseHub. Daarnaast ontvangen alle ISP's ook informatie van de NCSC met betrekking tot besmettingen. Daarnaast zijn er nog verschillende online sources waar informatie vandaan gehaald kan worden.	X		
	D-5	Ja	Ja	Ja	Ja	De ISP ontvangt informatie van de AbuseHub met betrekking tot besmettingen.	X		
ISP intern	D-6	Beperkt	Ja	Ja	Ja	De ISP heeft een aantal honeypots actief. Er wordt echter aangegeven dat dit een beperkte bijdrage levert aan botnetbestrijding.	X		
	D-7	Ja	Ja	Ja	Ja	Door de ISP wordt aangegeven dat er binnen een redelijke termijn zal worden gereageerd. Daarnaast wordt er aangegeven dat er niet op basis van slechts één melding actie wordt ondernomen. Meestal is dit een combinatie van meerdere meldingen.		X	

	D-8					Door de ISP worden een aantal systemen gebruikt om besmettingen te kunnen opsporen. Bijvoorbeeld aantal emails per seconde, DNS requests (dit is niet in één systeem). Dit zijn geen zogenaamde IDS oplossingen.			
Notificatie									
Klant	N-1	Ja	Ja	Ja	Ja	Door de ISP wordt er inzake een melding aan de klant onderscheid gemaakt tussen niet-zakelijke klanten en zakelijke klanten. Voor niet-zakelijke klanten bestaat de mogelijkheid dat ze in het geval van een besmetting in de walled garden omgeving geplaatst worden. Zakelijke klanten worden via email en de telefoon geïnformeerd in het geval van een besmetting.	X	X	
	N-2	Ja	Ja	Ja	Ja	De melding, die door de ISP aan de klant wordt verzonden, kan ook informatie bevatten omtrent tools en middelen om het probleem op te lossen.		X	
Andere partijen	N-3	Beperkt	Ja	Ja	Ja	Door de ISP wordt op beperkte schaal melding gedaan aan bijvoorbeeld andere providers.		X	
	N-4	Ja	Ja	Ja	Ja	De ISP geeft aan dat een bot bij een klant actief is en dus niet valt onder zijn zorgplicht. Door de ISP wordt aangegeven dat een ISP valt onder de zorgplicht en			

						meldplicht en dat dit ook botnets kunnen betreffen.			
Verwijdering/bestrijding									
Klant	V-1	Ja	Ja	Ja	Ja	De ISP heeft een walled garden omgeving actief.	X	X	
	V-2	Ja	Ja	Ja	Ja	Dit gebeurt door de vangpagina van de walled garden.		X	
	V-3	Nee				Door de ISP wordt aangegeven dat men bezig is de mogelijkheden hiervoor te onderzoeken.			
Klant / Andere partijen	V-4	Ja	Ja	Ja	Ja	Dit kan worden gedeeld binnen de vereniging Abuse information exchange.		X	
Andere partijen	V-5	Beperkt	Ja	Ja	Ja	Door de ISP wordt aangegeven dat het delen van best practices met betrekking tot verwijdering op beperkte schaal kan plaatsvinden.		X	
Herstel									
Klant	H-1	Ja	Ja	Ja	Ja	Door de ISP wordt aangegeven dat de klant zelf kan bepalen wanneer de klant weer online gaat. De walled garden vangpagina heeft een knop die de klant kan gebruiken om zijn verbinding weer te activeren.	X	X	
	H-2	Beperkt				Door de ISP wordt aangegeven dat dit op beperkte schaal kan plaatsvinden.		X	
	H-3	Beperkt				Door de ISP wordt aangegeven dat dit op beperkte schaal kan plaatsvinden.		X	

	H-4	Beperkt				Door de ISP wordt aangegeven dat dit op beperkte schaal kan plaatsvinden.		X	

Zijn er aspecten van botnetbestrijding die ISP's toepassen die ontbreken in het referentiemodel?
Nee
Welke aspecten zijn het meest effectief in de strijd tegen botnets op dit moment?
Door de ISP wordt aangegeven dat het gebruiken van een zogenaamde walled garden omgeving effectief is in de strijd tegen botnets.
Welke aspecten waren in het verleden effectief in de strijd tegen botnets?
Voor de AbuseHub werd er met name gereageerd op direct aan de ISP geadresseerde klachten (abuse meldingen). Nu is er een centraal systeem dat meldingen over besmettingen bij klanten verzamelt. Ook zijn er nu andere bronnen actief die samen in een Walled Garden systeem geautomatiseerd worden verwerkt, wat zorgt voor effectievere bestrijding van besmettingen.
Welke aspecten zijn volgens u effectief in de toekomst?
Het inzetten van de walled garden omgeving. Daarnaast de zorgplicht die ISP's hebben jegens hun klanten.

5. Niet ISP gerelateerde botnetbestrijdingsmethoden

In hoeverre klopt het dat bovenstaande voorstellen niet worden toegepast door ISP's?
Door de ISP wordt aangegeven dat de voorstellen uit de lijst niet worden toegepast.
Ontbreken hierin nog zaken?
Door de ISP wordt aangegeven dat de lijst compleet is.

Extra

Neemt de ISP maatregelen tegen degenen die het botnet beheren/aansturen, dus tegen de infectoren?
De ISP neemt geen maatregelen tegen degenen die het botnet aansturen, maar richt zich op zijn klant.

Uitwerking interviewverslag ISP5

Datum	9 september 2015
Plaats	-

1 Algemene vragen

1.1 Geïnterviewde

Wat is uw naam (incl. voorletters, evt. titels)?
-
Wat is uw functie/relatie tot botnetbestrijding?
-
Wat zijn uw belangrijkste taken, verantwoordelijkheden en bevoegdheden?
-
Voor welke Internet Service Provider werkt u?
-

1.2 Organisatie

Wat is de naam van de organisatie waarvoor u werkt?
-
Hoe is op hoofdlijnen de organisatie ingericht? Maakt de organisatie deel uit van een grotere organisatie?
-
Zijn er openbare publicaties beschikbaar, zoals rapporten en jaarverslagen, van en over uw organisatie waarin cyber security in het algemeen of botnetbestrijding aan bod komt?
Nee

2. Samenwerkingsverbanden

Bent u bekend met samenwerkingsverbanden op het gebied van botnetbestrijding?
De ISP is bekend met samenwerkingsverbanden.
Welke samenwerkingsverbanden inzake botnetbestrijding kent u?
De ISP is bekend met verschillende samenwerkingsverbanden zoals de vereniging Abuse Information Echange.
Aan welke samenwerkingsverbanden neemt uw organisatie deel? Zo ja, is dit een samenwerkingsverband binnen Nederland, Europa of wereldwijd.
De ISP neemt niet deel aan een samenwerkingsverband. Door de ISP wordt aangegeven dat hiervoor binnen de ISP niet genoeg mensen beschikbaar zijn. Echter, het is zeker een wens voor de toekomst.

3. Botnets

Welke definitie wordt binnen uw organisatie gehanteerd voor botnets?
Botnet is een netwerk van samenwerkende apparaten die zijn geïnfecteerd (onvrijwillig) met (dezelfde) malware en onder controle staan van een persoon of organisatie en die gecoördineerd cyberaanvallen kunnen uitvoeren.
Hoe worden botnets geclassificeerd?
Door de ISP wordt aangegeven dat een klant geïnfecteerd kan zijn of niet geïnfecteerd kan zijn. Er wordt niet specifiek een classificatie toegepast voor botnets.

4. Referentiemodel

Doelgroep	Aspect	Is dit aspect van toepassing voor uw organisatie?	Is de classificatie van het aspect juist? Zo nee, waarom niet en welke classificatie(s) is of zijn volgens u van toepassing op het aspect?	Is het aspect onderverdeeld in het juiste deelgebied? Zo nee, welk deelgebied is dan van toepassing en waarom?	Is het aspect toegekend aan de juiste doelgroep? Zo nee, welke doelgroep is dan van toepassing en waarom?	Opmerkingen	Technisch	Organisatorisch	Juridisch
Preventie									
Klant	P-1	Ja	Ja	Ja	Ja	De ISP biedt klanten de mogelijkheid om naast het bestaande abonnement een veiliginternet abonnement af te sluiten. De klanten kunnen dan onder andere gebruik maken van een virusscanner van F-secure.	X		
	P-2	Ja	Ja	Ja	Ja	Door de ISP wordt er actief gecommuniceerd met de klant door middel van een (periodieke) nieuwsbrief. In deze nieuwsbrief worden klanten gewezen op de risico's van het gebruik van internet. In de laatste nieuwsbrief wordt er dieper ingegaan op het instellen van een router wachtwoord en		X	X

						de beste encryptie voor draadloos internet.			
Andere partijen	P-3	Nee				Door de ISP wordt er geen informatie gedeeld omtrent botnetbestrijding.			
	P-4	Nee				Door de ISP wordt er op dit moment niet deelgenomen aan een samenwerkingsverband omtrent botnetbestrijding. Echter, de ISP geeft aan dat dit misschien in de toekomst wel gaat gebeuren.			
ISP intern	P-5	Wens	Ja	Ja	Ja	Door de ISP wordt aangegeven dat er geen IPS wordt gebruikt. Door de ISP wordt aangegeven dat het wel een wens is om een IPS in te zetten, maar dat zorgvuldig moet worden onderzocht wat hierin de juridische	X	X	

						mogelijkheden zijn in relatie tot netneutraliteit etc.			
	P-6	Ja	Ja	Ja	Ja	Door de ISP wordt aangegeven dat er technische maatregelen kunnen worden genomen en zijn genomen tegen botnets/malware.	X		
	P-7	Ja	Ja	Ja	Ja	De ISP volgt de laatste ontwikkelingen met betrekking tot botnets en malware. Dit kan zijn door het online bijhouden/lezen van informatie met betrekking tot botnets en malware. Echter, er worden geen specifieke trainingen met betrekking tot botnetbestrdijding gevolgd. Door de ISP wordt aangegeven dat hiervoor de resources ontbreken.	X		

	P-8	Ja	Ja	Ja	Ja	Binnnen de organisatie van de ISP zijn er klantsupport processen ingericht. Een voorbeeld hiervan is dat in het geval van een geconstateerde besmetting een procedure wordt gevolgd over de te nemen acties.	X		
	P-9	Ja	Ja	Nee, valt onder detectie. Omdat het abuse team actief wordt als een besmetting reeds is geconstateerd.	Ja	Binnen de ISP is een abuse team actief. Door de ISP wordt aangegeven dat het abuse team informatie van derden ontvangt over mogelijke besmettingen. De klant wordt in het geval van een besmetting via email/brief/telefoon geinformeerd.	X	X	
	P-10	Nee				De ISP maakt geen gebruik van Service Level agreements.			
	P-11	Nee				Op dit moment wordt geen gebruik gemaakt van ISO certificering.			
Detectie									
Klant	D-1	Nee				De ISP maakt geen gebruik van een self-identify portal.			

	D-2	Nee				Door de ISP wordt geen informatie ontvangen over besmettingen van klanten. De informatie over besmettingen komt in de meeste gevallen van externe bronnen.			
Andere partijen	D-3	Nee				De ISP deelt geen informatie over gedetecteerde besmettingen.			
	D-4	Ja	Ja	Ja	Ja	Door de ISP wordt informatie ontvangen van andere partijen zoals Shadowserver over mogelijke besmettingen binnen het netwerk van de ISP. Deze informatie wordt door ISP verwerkt en in het geval van een besmetting wordt er met de klant gecommuniceerd.	X		
	D-5	Nee				De ISP is op dit moment geen lid van de AbuseHUB.			
ISP intern	D-6	Nee				Door de ISP worden geen honeynets ingezet.			
	D-7	Nee				De ISP maakt geen gebruik van honeypots binnen het netwerk.			

	D-8	Wens	Ja	Ja	Ja	Door de ISP wordt geen gebruik gemaakt van een zogenaamde IDS. Voor dit aspect geldt het zelfde als P-5, namelijk dat dit een mogelijke wens is.	X		
Notificatie									
Klant	N-1	Ja	Ja	Ja	Ja	Indien een klant van de ISP is besmet, wordt de klant door middel van een brief/telefoon geinformeerd over de besmetting. Reageert de klant niet op de ISP, dan wordt in het extreme geval zijn verbinding afgesloten.		X	
	N-2	Ja	Ja	Ja	ja	De klant wordt door de ISP doorverwezen naar de veiliginternetten pagina van de ISP voor informatie.		X	
Andere partijen	N-3	Nee				Door de ISP wordt op dit moment geen melding gedaan aan andere providers.			
	N-4	Nee				Door de ISP worden botnetbesmettingen niet gemeld bij de ACM. Echter, de ISP is op de hoogte van de meldplicht in geval van datalekken.			
Verwijdering/bestrijding									

Klant	V-1	Nee				De ISP maakt geen gebruik van een zogenaamde 'walled garden'. Echter, indien een klant van de ISP besmet is, wordt zijn verbinding geisoleerd. De klant kan op dat moment geen gebruik meer maken zijn verbinding totdat hij aantoonbaar (door middel van bijvoorbeeld screenshot of logs) het probleem heeft opgelost. Binnen de ISP bestaat er wel de wens voor een 'walled garden' omgeving.			
	V-2	Ja	Ja	Ja	Ja	Door de ISP wordt aangegeven dat een klant hulp kan ontvangen inzake een botnetbesmetting als de klant contact opneemt met de helpdesk. De klant kan ook worden doorverwezen naar een lokale expert.	X	X	
	V-3	Ja	Ja	Ja	Ja	Indien een klant een probleem niet kan oplossen, kan de klant worden doorverwezen naar lokale partijen	X	X	

						waar hij professionele hulp kan inschakelen.			
Klant / Andere partijen	V-4	Nee				De ISP heeft geen walled garden omgeving actief.			
Andere partijen	V-5	Nee				De ISP deelt geen informatie omtrent botnetsmettingen met andere partijen.			
Herstel									
Klant	H-1	Ja	Ja	Ja	Ja	De ISP bepaalt wanneer de verbinding van de klant weer wordt geactiveerd.			
	H-2	Ja	Ja	Ja	Ja	Door de ISP wordt aangegeven dat de klant kan worden ondersteund in herstel. De ISP heeft de mogelijkheid voor een veilig internet abonnement. Darnaast geeft de ISP aan dat ondersteuning in herstel met betrekking tot botnets weinig voorkomt.		X	

	H-3	Ja	Ja	Ja	Ja	Op het moment dat een besmetting wordt geconstateerd bij een klant wordt de klant door middel van een waarschuwingsbrief hierover geinformeerd. Hierin staat informatie over mogelijke gevolgen van herstel met betrekking tot persoonlijke data en accounts.		X	
	H-4	Nee				De ISP geeft geen informatie over hoe herstel kan plaatsvinden.			

Zijn er aspecten van botnetbestrijding die ISP's toepassen die ontbreken in het referentiemodel?
Door de ISP wordt aangegeven dat er in het referentiemodel geen zaken ontbreken.
Welke aspecten zijn het meest effectief in de strijd tegen botnets op dit moment?
Door de ISP wordt aangegeven dat het delen van informatie rond besmettingen effectief werkt. Daarnaast is het ook van belang klanten bewust te maken van de gevaren op het internet en tips te geven.
Welke aspecten waren in het verleden effectief in de strijd tegen botnets?
Virusscanners
Welke aspecten zijn volgens u effectief in de toekomst?
Door de ISP wordt aangegeven dat samenwerken tussen bijvoorbeeld ISP's en overheid in de strijd tegen botnets effectief kan zijn in de toekomst. Maar ook zaken zoals walled garden en inzetten op preventie.

5. Niet ISP gerelateerde botnetbestrijdingsmethoden

In hoeverre klopt het dat bovenstaande voorstellen niet worden toegepast door ISP's?
Door de ISP wordt aangegeven dat genoemde voorstellen niet worden toegepast. Het kan heel af en toe voorkomen dat er een website wordt geblokkeerd (ISP intern).
Ontbreken hierin nog zaken?
Nee

6. Opmerkingen

Extra
De ISP neemt waar mogelijk technische maatregelen tegen malware/botnets. De ISP heeft bijvoorbeeld een limiet op het aantal te versturen emails per uur en monitort hierop in zijn netwerk. Door de ISP wordt aangegeven dat het toetreden tot een samenwerkingsverband een wens is. Ondanks dat de ISP op dit moment geen onderdeel is van een samenwerkingsverband ontvangt de ISP van verschillende resources informatie over mogelijke besmettingen. Indien de ISP geattendeerd wordt over een mogelijke besmetting kan hij de klant isoleren door zijn verbinding daadwerkelijk stop te zetten totdat de klant aangeeft de besmetting te hebben opgelost. Met de klant wordt via email en post gecommuniceerd.
Neemt de ISP maatregelen tegen degenen die het botnet beheren/aansturen, dus tegen de infectoren?
Door de ISP wordt aangegeven dat er alleen acties worden ondernomen tegen bots. Het ondernemen van acties tegen botnetstructuren en botmasters is een taak die is weggelegd voor de overheid.

Uitwerking interviewverslag NCSC

Datum	25-9-2015
Plaats	Den Haag

2 Algemene vragen

2.1 Geïnterviewde

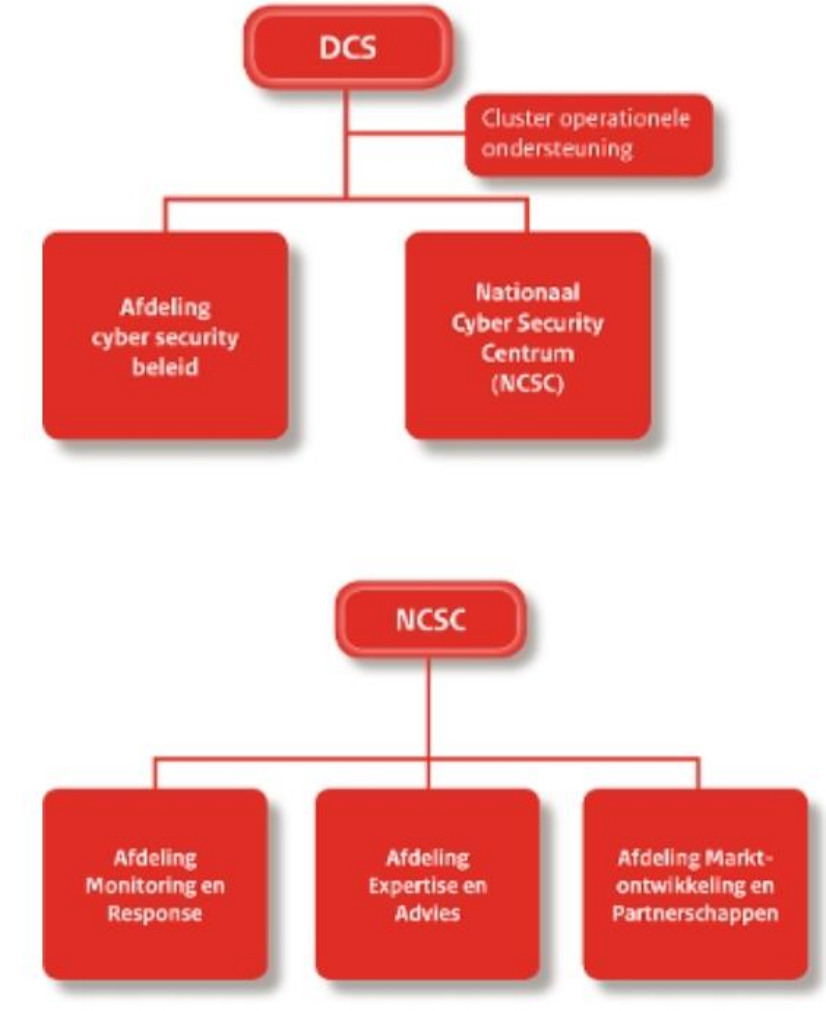
Wat is uw naam (incl. voorletters, evt. titels)?
-
Wat is uw functie/relatie tot botnetbestrijding?
Adviseur van het NCSC op het gebied van Cybersecurity.
Wat zijn uw belangrijkste taken, verantwoordelijkheden en bevoegdheden?
Beantwoorden van specifieke adviesvragen vanuit de doelgroep van het NCSC Begeleiden projecten Publicaties website/presentaties
Voor welke organisatie werkt u?
Nationaal Cyber Security Centrum (NCSC)

2.2 Organisatie

Wat is de naam van de organisatie waarvoor u werkt?

NCSC

Hoe is op hoofdlijnen de organisatie ingericht? Maakt de organisatie deel uit van een grotere organisatie?



Het valt onder het ministerie van Veiligheid en Justitie.

Zijn er openbare publicaties beschikbaar, zoals rapporten en jaarverslagen, van en over uw organisatie waarin cyber security in het algemeen of botnetbestrijding aan bod komt?

Op de website van het NCSC zijn meerdere publicaties over security en botnetbestrijding terug te vinden. Door het NCSC wordt sinds 2011 elk jaar het Cybersecuritybeeld gepubliceerd.

7. Samenwerkingsverbanden

Bent u bekend met samenwerkingsverbanden op het gebied van botnetbestrijding?

Het NCSC is bekend met samenwerkingsverbanden op het gebied van botnetbestrijding.

Welke samenwerkingsverbanden inzake botnetbestrijding kent u?

Abusehub ACDC CAT 5 BotLEG NRN EMPACT-project AbuseNL Veiligbankieren.nl Veiliginternetten.nl AlertOnline ShadowServer
Aan welke samenwerkingsverbanden neemt uw organisatie deel? Zo ja, is dit een samenwerkingsverband binnen Nederland, Europa of wereldwijd.
Er zijn diverse samenwerkingsverbanden waar het NCSC aan mee werkt. Sommige hiervan zijn geheim en besloten.

8. Botnets

Welke definitie wordt binnen uw organisatie gehanteerd voor botnets?
De algemeen geldende definitie wordt gehanteerd binnen het NCSC (geen eigen definitie binnen het NCSC).
Hoe worden botnets geclassificeerd?
Geen eigen classificatie. Er wordt gebruik gemaakt van de algemeen geldende definities. Dus bijvoorbeeld fast flux of dga botnets.

9. Referentiemodel

Het referentiemodel is met het NCSC geëvalueerd. Echter, is het voor het NCSC lastig om aan te geven wat er moet gebeuren of zou moeten gebeuren in de strijd tegen botnets. Het NCSC kan niemand ergens toe verplichten. Het NCSC beschikt niet over een wettelijk mandaat. Door het NCSC wordt aangegeven dat alles, wat er gebeurt om botnets te voorkomen of te bestrijden binnen het wettelijke kader, positief is. Door het NCSC is aangegeven dat het referentiemodel compleet en correct is. Er zijn echter een aantal zaken die niet worden gedaan door ISP's. Dit zijn P-5, P-10. D-8 en N-4. Vervolgens is de lijst doorgenomen en is er een score toegekend aan de verschillende aspecten en is gekeken of een aspect technisch, organisatorisch of juridisch van aard is.

Doelgroep	Aspect	Naam kenmerk	Omschrijving	Technisch	Organisatorisch	Juridisch	Score
Preventie							
Klant	P-1	Beschikbaar stellen end-point security	ISP's stellen end-point security oplossingen beschikbaar voor hun klanten. Dit kan bijvoorbeeld door klanten een antivirussoftware aan te bieden of een router met beveiliging.	x	x		5
	P-2	Educatie van klanten	Door ISP's wordt er actief uitleg gegeven over het gevaar van botnets en de acties die klanten kunnen ondernemen om dit te voorkomen. Hierbij valt te denken aan: waarom klanten hun software up-to-date moeten houden, bewustwording campagnes, aanmoedigen van klanten om een end-point security oplossing te gebruiken, belang van backups en acties die klanten kunnen ondernemen om niet onderdeel te worden van een botnet. Eén van de doelen van educatie van klanten is de volgende: dat er bij de klant bewustwording ontstaat dat hij mede verantwoordelijk is in het voorkomen van een botnetbesmetting (gedeelde verantwoordelijkheid).	x	x	x	5

Andere partijen	P-3	Delen/communiceren van informatie/procedures omtrent botnetbestrijding	Door ISP's wordt er actief gecommuniceerd met andere stakeholders zoals ISP's. Door ISP's wordt bijvoorbeeld informatie gedeeld met andere stakeholders over lessons-learned en procedures inzake botnetbestrijding.		x		4
	P-4	Deelnemen in een samenwerkingsverband inzake botnetbestrijding	Door ISP's wordt actief deelgenomen in samenwerkingsverbanden met betrekking tot botnetbestrijding.		x		5
ISP intern	P-5	Intrusion Prevention Systems (IPS)	ISP's maken gebruik van Intrusion Prevention Systems (IPS) om botnetbesmettingen te kunnen voorkomen.	x			
	P-6	Nemen van technische maatregelen inzake botnets	ISP's kunnen een aantal technische maatregelen nemen zodat het moeilijker wordt voor een botnet om machines te infecteren. Bijvoorbeeld het beveiligen van DNS servers.	x			5
	P-7	Bijhouden stand van zaken met betrekking tot botnet/malware technieken.	ISP's blijven op de hoogte van de laatste ontwikkelingen met betrekking tot botnets en malware. Bijvoorbeeld door het trainen van personeel met betrekking tot bestrijding en detectie van botnets.	x	x		3
	P-8	Klant support processen	Door de ISP's zijn er processen ingericht omtrent klantondersteuning inzake botnetbesmettingen.		x		3
	P-9	Abuse team	ISP's hebben een abuse team actief.		x		3
	P-10	Service Level Agreements	ISP's richten Service Level Agreements in met betrekking tot botnetbestrijding.		x		
	P-11	Standaardisering	Voldoen aan internationale standaarden inzake beveiliging (ISO 27002:2005, ISO 27006:2007)		x		1
Detectie							
Klant	D-1	Aanbieden self-identify portal	Gebruikers zelf via tools, web portal of andere resource een mogelijke infectie laten vaststellen		x		5
	D-2	Ontvangen informatie over mogelijke besmettingen via klanten	ISP's kunnen van klanten informatie krijgen over besmettingen binnen hun netwerk.		x		2

Andere partijen	D-3	Communiceren gedetecteerde besmettingen	ISP's delen informatie over gedetecteerde besmettingen met andere ISP's.		x		4
	D-4	Ontvangen informatie over mogelijke besmettingen via externe partijen	ISP's kunnen informatie over kwaadaardige activiteiten en bot geïnfecteerde klanten krijgen van externe partijen.		x		4
	D-5	Ontvangen informatie over mogelijke besmettingen via AbuseHUB	ISP's ontvangen informatie over mogelijke besmettingen vanuit het AbuseHUB systeem.		x		5
ISP intern	D-6	Honeynet	ISP's maken gebruik van honeypots om besmettingen in het netwerk te kunnen constateren.	x			4
	D-7	Detectie besmetting	Als een besmetting wordt geconstateerd, of daarop wordt gewezen door een derde, zal de ISP binnen een redelijke termijn beoordelen of hij hier tegen moet optreden.	x			3
	D-8	Intrusion Detection Systems (IDS)	ISP's maken gebruik van Intrusion Detection Systems (IDS) om botnetbesmettingen te kunnen constateren (bijvoorbeeld door monitoring).	x			
Notificatie							
Klant	N-1	Melding aan geïnfecteerde klanten	Gebruiker informeren over een mogelijke besmetting Dit kan via email, telefoon, in-browser, instantmessaging, SMS of via walled garden bericht.		x		5
	N-2	Koppeling melding met remediation tools	De melding die de gebruiker in geval van besmetting ontvangt, bevat ook informatie over tools en middelen om het probleem op te lossen.	x	x		5
Andere partijen	N-3	Melding aan andere providers	ISP's melden besmettingen aan andere providers.		x		4
	N-4	Melding ACM	ISP's zijn verplicht om in bepaalde omstandigheden een melding te doen bij de autoriteit ACM.		x	x	
Verwijdering/bestrijding							
Klant	V-1	Isoleren gebruiker	Het plaatsen van geïnfecteerde gebruikers in een zogenaamde 'walled garden'.	x	x		5

	V-2	Delen van informatie omtrent het oplossen van een botnetinfectie	ISP's stellen informatie beschikbaar hoe klanten een mogelijke botnetinfectie kunnen oplossen.	x	x		5
	V-3	Links naar professionele hulp	De ISP kan klanten informatie geven over waar de klant professionele hulp kan vragen.		x		4
Klant / Andere partijen	V-4	Delen procedure walled garden	De procedure rond het isoleren van besmettingen (walled garden) wordt gedeeld met klanten en andere ISP's zodat voor klanten duidelijk is wanneer zij weer gebruik van hun verbinding kunnen maken.		x		3
Andere partijen	V-5	Delen best practices verwijdering	ISP's delen informatie met betrekking tot het verwijderen van botnets met andere instanties.		x		3
Herstel							
Klant	H-1	Activeren verbinding klant	De ISP bepaalt op welk moment en hoe een consument weer gebruik kan maken van de internetverbinding nadat de besmetting is verwijderd.	x	x		4
	H-2	Ondersteunen van klanten in herstel	ISP's stellen informatie over remediation beschikbaar (dit kan via publicaties of web links) over hoe een klant een botnetinfectie kan oplossen.		x		4
	H-3	Gevolgen herstel met betrekking tot persoonlijke data en accounts	De ISP informeert de klant welke gevolgen het oplossen van een besmetting heeft met betrekking tot persoonlijke bestanden.		x		3
	H-4	Informatie herstel	ISP's stellen informatie beschikbaar die klanten kunnen helpen in het herstellen van hun data na het oplossen van een botnetbesmetting.		x		3

Zijn er aspecten van botnetbestrijding die ISP's toepassen die ontbreken in het referentiemodel?
Het model is volledig.
Welke aspecten zijn het meest effectief in de strijd tegen botnets op dit moment?
Door het NCSC wordt aangegeven dat slachtoffernotificatie een belangrijke rol kan spelen bij het bestrijden van een botnet.
Welke aspecten waren in het verleden effectief in de strijd tegen botnets?
Het uit de lucht halen van een zogenaamde C&C server.
Welke aspecten zijn volgens u effectief in de toekomst?
Slachtoffernotificatie.

10. Niet ISP gerelateerde botnetbestrijdingsmethoden

In hoeverre klopt het dat bovenstaande voorstellen niet worden toegepast door ISP's?
De in de lijst genoemde items worden niet door ISP's toegepast.
Ontbreken hierin nog zaken?
Nee.

11. Opmerkingen

Extra
Tussen het NCSC en de ISP's is operationeel contact inzake botnetbestrijding. De grotere ISP's hebben vaak een incident response team actief en zijn er directe lijnen met het NCSC. Door het NCSC wordt niet deelgenomen aan de Vereniging Abuse Information Exchange, maar het NCSC kan wel data over mogelijke besmettingen leveren aan de vereniging. Het NCSC vervult een centrale rol met het verspreiden van informatie rond botnetbesmettingen. Door de adviseur van het NCSC wordt aangegeven dat slachtoffernotificatie het beste middel is in de strijd tegen botnets. Dit komt op het volgende neer. Wanneer een infectie bij een ISP wordt gemeld, zal de ISP's actie ondernemen door de klant te isoleren en te notificeren. Volgens het NCSC zijn ISP's een logisch centraal punt om een botnet te bestrijden. Echter, er is in de gemeenschap geen consensise over wie de verantwoordelijkheid in botnetbestrijding op zich moet nemen.
Neemt de ISP maatregelen tegen degenen die het botnet beheren/aansturen, dus tegen de infectoren?
Door het NCSC wordt aangegeven dat ISP's maatregelen nemen tegen bots en niet zozeer tegen de commandostructuur of degene achter het botnet.